EXHIBIT 17

Redacted Version of Document Sought to be Sealed

Brown v. Google

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA

	§	
	§	
	§	
CHASOM BROWN, WILLIAM BYATT,	§	
JEREMY DAVIS, CHRISTOPHER	§	
CASTILLO, and MONIQUE TRUJILLO,	§	
individually and on behalf of all similarly	§	
situated,	§	
	§	
	§	**Case No. 4:20-cv-03664-YGR-SVK**
Plaintiffs,	§	
v.	§	
	§	
	§	
GOOGLE LLC,	§	
	§	
Defendant.	§	
	§	
	§	
	§	
	§	
	§	

EXPERT REBUTTAL REPORT OF BRUCE SCHNEIER

REBUTTAL OF EXPERT GEORGIOS ZERVAS

June 7, 2022

Brown v. Google

TABLE OF CONTENTS

Brown v. Google

I.   Executive Summary of Opinions

1.   Pursuant to the Court's Standing Order, this section includes an executive summary of each option to be proffered in this rebuttal report. My opinions include:

A. OPINION 1: As described in Section III.1, Professor Zervas erred by failing to address evidence produced by Google in this case (including evidence cited in my opening report) regarding how Google collects and stores private browsing information, which makes Professor Zervas' stated opinions incomplete and misleading.

B. OPINION 2: As described in Section III.2, contrary to what Professor Zervas suggests in his report and consistent with the opinions stated in my opening report, the private browsing information collected and stored by Google can be linked with devices and users, and Professor Zervas erred by only considering cookie values associated with private browsing and by failing to address the joinability implications of other information collected by Google during private browsing.

C. OPINION 3: As described in Section III.3, despite being retained by Google, Professor Zervas has not presented any analysis regarding or established any widespread awareness or use during private browsing of any of the "other settings and available features" he discusses, and it is my experience and opinion that ordinary Internet users do not know about, do not know how to use, or do not know that it might be advisable to use these "other settings and available features" during private browsing.

D. OPINION 4: As described in Section III.3, Professor Zervas fails to address how Google's marketing of private browsing mode serves as a control that prevents Google from collecting and saving users' private browsing data undermines users' motivation to discover or learn how to use the "other settings and available features" that Professor Zervas identifies.

E. OPINION 5: As described in Section III.4, Professor Zervas fails to address how Google has financial incentives to collect as much data and information as it possibly can and to make it difficult for users to escape Google's tracking beacons, and that Google is therefore incentivized to steer users toward a "private" browsing mode rather than any settings or features that might impact its collection of browsing data.

F. OPINION 6: As described in Section III.5, Professor Zervas fails to account for how Google's persistence in referring to Incognito mode as a "private" browsing (both before and throughout the class period) mode has exacerbated users' misconceptions of what Professor Zervas claims to be the sole purpose of private browsing (that is, to ensure that others who use the same device cannot see the user's activity), and Professor Zervas is wrong to suggest that private browsing modes work as described in public documentation.

Brown v. Google

II.   <u>**Background**</u>

2.   Counsel for the Plaintiffs in this action ("Counsel") retained me to provide certain opinions concerning issues of privacy and the alleged conduct. On April 15, 2022, I submitted a report in which I analyzed issues relating to Google's disclosures and practices, the private browsing modes at issue, reasonable privacy expectations, whether certain practices could be highly offensive or constitute a serious invasion of privacy, and issues relating to the value of privacy and user data ("Opening Schneier Report").

3.   The Opening Schneier Report contained a section outlining my expertise, and my detailed CV was included as Appendix 2 to that report.[1]

4.   Counsel has also asked me to review the Expert Report of Professor Georgios Zervas, submitted by Google on April 15, 2022 ("Zervas Report") and to render any opinions that I have concerning it. I have reviewed the Zervas Report and all of the materials appended to it.

5.   As before, I am compensated at the rate of $675/hour and my research associate, Kathleen Seidel, is being compensated at the rate of $75/hour. Our compensation does not depend upon the outcome of the case. In the event of any recovery in this case, I understand that Ms. Seidel and I will be excluded from any disbursement of funds.

6.   In preparing this rebuttal report, I have relied upon the documents identified herein, which are listed in Appendix 1. As part of my research, Ms. Seidel and I had access to a database containing tens of thousands of confidential Google documents that Google produced during the discovery process in this case and marked "Confidential." These documents were fully sufficient to support my opinion in this case. We did not request and were not provided access to documents designated "Highly Confidential—Attorneys' Eyes Only." My understanding is that such documents generally concern a level of technical detail that was unnecessary for me to consider in forming the opinions I have expressed in this case. I used the ILS document review platform to search for relevant documents. Ms. Seidel and I had free rein to conduct our own searches within this database of "Confidential" documents. We also had access to Google's Interrogatory and Request for Admission responses, except for any materials marked as "Highly Confidential—Attorneys' Eyes Only." Finally, we had access to all deposition transcripts, except for portions that were redacted, which I understand were portions deemed by Google to be "Highly Confidential—Attorneys' Eyes Only." We also had access to all of the named plaintiffs' deposition transcripts.

7.   Like my opening report, this report has been prepared for purposes of this case only. It may not be used for any other purpose. This report contains and refers to information designated as "Confidential" under a Stipulated Protective Order, to which Ms. Seidel and I have agreed to be bound. Neither of us has reviewed or relied on any discovery produced by Google marked as "Highly Confidential—Attorneys' Eyes Only." Those were not accessible to us.

---

[1] Opening Schneier Report ¶¶ 6-20.

Brown v. Google

III.   <u>Opinions</u>

1.   **Professor Zervas failed to investigate Google's systems or engage with the actual evidence in this case.**

8.   Professor Zervas asserts that the "sources [he] considered in forming [his] opinions are identified in [his] report and the accompanying exhibits and are listed in the attached Appendix C."[2] Appendix C includes only a small selection of what he labels "Case Documents." That includes the Third Amended Complaint and deposition testimony of eight Google employees.

9.   Professor Zervas provides no explanation for why he only considered the materials identified in Appendix C, without any further investigation and analysis.

10.   As an expert retained by Google's counsel, I assume that Professor Zervas could have easily obtained access to Google employees and details about how their systems work, and yet I see no evidence in his report that he took the opportunity to learn more about how Google actually stores and uses private browsing information, which is the subject of this lawsuit.

11.   In addition, Professor Zervas failed to contend with the thousands of documents produced by Google in this lawsuit, where, for example (and as detailed in my Opening Report), Google employees readily admit that Google can link private and non-private browsing data.

12.   With my research assistant Ms. Seidel, we spent many hours searching Google's productions and reviewing deposition transcripts to address the actual evidence in this case. Professor Zervas does not seem to have undertaken any of that important work. As a result, as explained below, Professor Zervas presents opinions that are in many respects directly contrary to and undermined by other evidence in this lawsuit, which in turn supports my opinions. It is my further opinion that Professor Zervas's failure to consider the larger body of relevant materials available to him is not consistent with professional standards of rigor in the fields of computer science, security, data privacy, and human factors, which makes his opinions as a whole uninformed, misleading, and unreliable.

2.   **Contrary to Professor Zervas's assertions, private browsing information collected and stored by Google can be linked with devices and users.**

13.   Professor Zervas asserts that "Private Browsing Modes ensure that cookie values generated during the Private Browsing Session cannot be used to provide a link to the user or her device after the session is closed."[3]

14.   He states: "Because cookie values associated with Private Browsing Sessions are not shared with other browsing sessions, this information cannot be used to link the Private Browsing Mode activity to a user or her device after that Private Browsing Session is closed."[4]

---

[2] Zervas Report ¶ 19.

[3] Zervas Report ¶ 2.

[4] Zervas Report ¶ 6.

Brown v. Google

15.   He continues: "The cookie value transmissions to Google-associated domains—when a user who is not logged into a Google account and uses Private Browsing Mode to visit a third-party website containing 'Google tracking or advertising code'—constitute 'orphaned' islands of data that cannot be used to provide a link to a user's Google Account or other Private Browsing Sessions."[5]

16.   Although Professor Zervas discusses cookies at length, an Internet cookie is just one datapoint collected or placed by Google's tracking beacons; that is, code embedded in web pages that collects data about the user's activity, and relays data to a surveillance company's website (e.g., an advertising network such as Google's).

17.   Professor Zervas's analysis is incomplete, which makes his report misleading. He errs by only considering information "saved on the device" and "cookie values," and failing to address the implication for joinability of other data that Google collects, including from users' private browsing.

18.   As one example of his incomplete analysis, Professor Zervas provides no analysis of browser fingerprinting. The word "fingerprint" appears just three times in his entire report, and each instance is just quoted material from the Plaintiffs' Complaint.[6] Professor Zervas does not attempt to explain or address fingerprinting, nor its relevance to this case.

19.   As explained in one recent article, "Whenever you go online, your computer or device provides the sites you visit with highly specific information about your operating system, settings, and even hardware. The use of this information to identify and track you online is known as device or browser fingerprinting."[7]

20.   The Electronic Frontier Foundation explains it this way: "A digital fingerprint is essentially a list of characteristics that are unique to a single user, their browser, and their particular hardware setup. This includes information the browser needs to send to access websites, like the location of the website the user is requesting. But it also includes a host of seemingly insignificant data (like screen resolution and installed fonts) gathered by tracking scripts. Tracking sites can stitch all the small pieces together to form a unique picture, or 'fingerprint,' of your device."[8] This sentence might sound less weird if you turned it around: Plugins, cookie preferences, and ad blockers also generate information that can be used to fingerprint browsers.[9]

21.   Professor Zervas fails to consider Google's own internal documents that similarly describe fingerprinting as "the use of unique or probabilistically unique combinations of one or more device, network or app/browser attributes to identify a device, app, browser, or user across

---

[5] Zervas Report ¶ 83.

[6] Zervas Report ¶¶ 14, 16.

[7] Sven Taylor (23 Feb 2022), "Browser fingerprinting protection: How to stay private," Restore Privacy, https://restoreprivacy.com/browser-fingerprinting.

[8] Electronic Frontier Foundation (2020), "How do trackers work?" *Cover Your Tracks*, https://coveryourtracks.eff.org/learn.

[9] Sven Taylor (23 Feb 2022), "Browser fingerprinting protection: How to stay private," *Restore Privacy*, https://restoreprivacy.com/browser-fingerprinting.

Brown v. Google

different transactions where no persistent unique identifier is explicitly provided by a user's device, app, or browser."[10]

22.   Google apparently uses fingerprinting in particular scenarios, such as fraud prevention and information security.[11] This means there are instances in which Google employees would be allowed to join a user's private browsing data with his or her device or name, at least for those specific purposes.

23.   Of course, whether Google currently permits browser fingerprinting (regardless of whether Google's policy limits its use to certain circumstances) is really beside the point. As I explained in my opening report, users' online "privacy concerns are justified by the volume and scope of data generated, collected, and used when people access the Internet and by the potential for such data to reveal sensitive information about individual users."[12]

24.   A recent case-in-point is the Supreme Court's apparent intention to overturn *Roe v. Wade*, and the efforts in some states to prosecute women who seek abortions in other states.[13] It has been reported that a company named SafeGraph has been selling data about people traveling to and from abortion clinics.[14] Legislators have insisted that Google stop collecting and storing "unnecessary" location data due to the risk that law enforcement in states that newly criminalize abortion might seek to access Google's records to identify women who have sought information about abortion clinics.[15] Another worrisome example is Immigration and Customs Enforcement's reported efforts to track undocumented immigrants through deals with data brokers.[16]

25.   These examples call to mind an August 2019 Google document that I highlighted in my opening report, in which Google employees recognized that "we know that users today don't

---

[10] GOOG-BRWN-00029326 at -26.

[11] GOOG-BRWN-00842731 at -35.

[12] Opening Schneier Report, Opinion 3.

[13] Melody Schreiber (3 May 2022), "US states could ban people from traveling for abortions, experts warn," *Guardian*, https://www.theguardian.com/world/2022/may/03/us-abortions-travel-wave-of-restrictions.

[14] Joseph Cox, "Data broker is selling location data of people who visit abortion clinics," *Vice*, https://www.vice.com/en/article/m7vzjb/location-data-abortion-clinics-safegraph-planned-parenthood (May 3, 2022).

Geoffrey A. Fowler and Tatum Hunter, "Your phone could reveal if you've had an abortion," *Washington Post*, https://www.washingtonpost.com/technology/2022/05/04/abortion-digital-privacy (May 4, 2022).

[15] Corin Faife, "Democrats say Google must curb location tracking before Roe repeal," *The Verge*, https://www.theverge.com/2022/5/24/23140279/democrat-letter-google-location-data-abortion-surveillance-geofence-warrants (May 24, 2022).

Barbara Ortutay, "Democrats: Google must protect privacy of abortion patients," Associated Press, https://apnews.com/article/abortion-technology-health-patient-privacy-f5d03037cec832160c450d24b026701d.

[16] Corin Faife (10 May 2022), "ICE uses data brokers to bypass surveillance restrictions, report finds," The Verge, https://www.theverge.com/2022/5/10/23065080/ice-surveillance-dragnet-data-brokers-georgetown-law.

Brown v. Google

fully understand the privacy protections that Incognito (IM) provides, potentially putting users at risk in the moments when they expect the most privacy."[17]

26.   It is apparent that Google collects and stores private browsing data that can be used for fingerprinting. In a March 2010 email exchange, occurring soon after Incognito was first developed and offered to the public in 2008, Google employees discussed an external article that addressed "browser fingerprinting."[18] One Google employee characterized the issues it addressed as "just the tip of the iceberg." He continued: "I can profile you with your installed plugins, font list (exposed via plugins), etc. Not to mention your IP." That "iceberg" is fingerprinting, which Google can readily accomplish with private browsing data.

27.   Google's internal documents demonstrate that its ability to fingerprint users persisted into the class period of this case. An internal document from September 2018 titled, "Incognito Mode, Current and Possible Promises," notes (as mentioned in my opening report) that while "Incognito mode and regular mode should not be linkable...This is to some extent violated by fingerprinting."[19] That observation was correct; the data from Incognito mode and regular mode is linkable through fingerprinting.

28.   And in a December 2019 document titled, "How to lead in a privacy-first era," a Google software developer explained how "fingerprinting techniques rely on collecting several unique attributes about a user's device such as operating system, browser version, browser language, fonts installed, screen resolution and more. Combined, those details create a unique profile of a user's device and, by proxy, the user. Users can't see that this data is being collected, nor can they delete it by clearing cookies. Fingerprinting ignores any privacy choices that a user may have previously made, and they cannot opt-out of it (even if they are aware of it)."[20]

29.   This explanation underscores how Professor Zervas misses the point, and how his opinions regarding linking based on cookies are misleading. Whether cookies are discarded from the browser has no bearing on whether the plethora of data that Google has already been collecting can be used for fingerprinting—or whether Google can join a person's regular and Incognito browsing data. While Professor Zervas suggests otherwise, the documents produced by Google (and ignored by Professor Zervas) support my opinions regarding linkability.

30.   Another internal Google document reinforces Professor Zervas's error: "Fingerprinting is worse than cookies in some aspects: (1) fingerprinting normally doesn't store anything onto your computer, so you can't clear or reset the tracking data, (2) fingerprinting is done silently without the users' consent."[21] Indeed, "fingerprints can be used to fully or partially identify individual users or devices even when persistent cookies...can't be read or stored in the browser, the client IP address is hidden, and even if one switches to another browser on the same device."[22]

---

[17] GOOG-BRWN-00569625 at -26.

[18] GOOG-BRWN-00848778 at -80.

[19] GOOG-BRWN-00047390 at -392.

[20] GOOG-BRWN-00026989 at -92.

[21] GOOG-CABR-04006287 at -88.

[22] GOOG-CABR-04006287 at -87.

Brown v. Google

Moreover, "browser fingerprinting does not leave any trace as it does not require the storage of information inside the browser."[23]

31.   Other specific examples of information that can be used to join private browsing data to users and their devices, which Professor Zervas likewise does not assess, include IP addresses and user agent information, as well as identifiers tied to users' accounts with non-Google websites.

32.   Professor Zervas's analysis further misses the point with respect to Google's collection of IP addresses from Incognito users who visit non-Google websites. Although he recognizes that Google collects that information, as well as the importance of anonymizing and/or masking IP address information, he neglects to consider the implications of Google's collection of IP address information for purposes of joinability.

33.   Professor Zervas repeatedly acknowledges that Google collects the IP addresses of private browsing users who visit non-Google websites.[24] He also describes Google Analytics's "offer [...] [to] customers the option to anonymize users' IP addresses" as one example of how "Google Analytics customers have control over whether Google collects and uses data relating to users' interactions with the customer's website."[25]

34.   But Professor Zervas fails to clarify that "Google Analytics customers" are not the users of the Chrome browser, but instead the companies whose websites Chrome browser users are visiting. His assurance provides no comfort to those users, who are offered no control within the browser over the configuration of their IP address on websites' server logs, whether they are browsing in regular or Incognito mode. Further, he does not describe any option for those Google Analytics customers to anonymize users' IP addresses only for private browsing.

35.   Professor Zervas suggests that "VPN services are an effective tool to mask users' IP addresses and would prevent the user's true IP address from being sent in transmissions to Google-associated domains,"[26] reiterating the significance of the IP address as a form of sensitive personal information. This incorrectly assumes, however, that users would understand the need to mask their IP addresses even during private browsing. It also ignores the many other kinds of data Google collects that may be used to fingerprint private browsing users.

36.   Professor Zervas also ignores Google's March 2022, announcement that Google Analytics 4 will "no longer store IP addresses."[27] Google deemed this change "necessary" because "users

---

[23] GOOG-BRWN-00554517 at -18.

[24] Zervas Report ¶ 7, 9, 46, 94.

[25] Zervas Report ¶ 94, 98.

[26] Zervas Report ¶ 147.

[27] Russell Ketchum (16 Mar 2022), "Prepare for the future with Google Analytics 4," Google Marketing Platform, https://blog.google/products/marketingplatform/analytics/prepare-for-future-with-google-analytics-4.

James Hercher (16 Mar 2022), "Google Analytics to stop logging IP addresses and sunset old versions in privacy standards overhaul," Ad Exchanger, https://www.adexchanger.com/online-advertising/google-analytics-to-stop-logging-ip-addresses-and-sunset-old-versions-in-privacy-standards-overhaul.

Brown v. Google

are increasingly expecting more privacy protections and control over their data." That Google associates no longer collecting IP addresses with "more privacy" is telling. Google recognizes the joinability risk posed by the collection of IP address information. Given the limited information included in Google's announcement, it is not possible at this point to assess the full extent to which Google will "no longer store IP addresses" and how that may in the future provide some additional privacy to users of private browsing modes.

37.   Another important tool for joinability is the user agent string. Yet the phrase "user agent" appears only once in the entire Zervas Report, in a sentence acknowledging that Google receives this information from users' private browsing.[28] Although Professor Zervas characterizes the User Agent Request Header as a means of "inform[ing] the server about the web browser [...] to improve browsing experience," user agent data also includes information about a user's operating system, and can be used to personally identify the user.[29] Professor Zervas nowhere grapples with the ramifications of Google's collection and storage of user agent strings, let alone the combination of user agent and IP address.

38.   As I explained in my opening report, "In an August 8, 2019, email, a Google developer noted that, 'To be perfectly clear, the data collected while Incognito is strictly **NOT** anonymous. [emphasis in original] When using a Google service, data (e.g., search queries) is tied to a pseudonymous ID [...] that is then stored with the user's IP address, user agent and other metadata (everything in the gwslog proto). While we don't connect it to a user's identity and there are many internal policies to ensure it does not happen, it's not impossible. [...] we potentially might be continuously trying to stay ahead, while making privacy worse by collecting Incognito when the user has clearly told Chrome that it wants to be private.'"[30] Professor Zervas nowhere cites or addresses this internal Google email.

39.   As I also explained in my opening report, "even if Google is not building user profiles across signed-in and signed-out data, Google's decision to collect and log this data creates the potential for data to be joined in this way. For example, Google's storage of unique identifiers and IP addresses together in logs introduces a risk that data from a users' private browsing will

---

Kendra Clark (16 Mar 2022), "Google Analytics stops logging IP addresses: here's why it's a big deal for marketers," The Drum, https://www.thedrum.com/news/2022/03/16/google-analytics-nixes-ip-address-logging-new-privacy-play.

[28] Zervas Report ¶ 34.

[29] Peter Eckersley, "How unique is your web browser?" Proceedings of the 10th International Conference on Privacy Enhancing Technologies, Berlin, https://coveryourtracks.eff.org/static/browser-uniqueness.pdf (July 2010).

See also:

Nick Nikiforakis, et al., "Cookieless monster: Exploring the ecosystem of web-based device fingerprinting," 2013 IEEE Symposium on Security and Privacy, 2013, https://ieeexplore.ieee.org/abstract/document/6547132 (May 19, 2013).

Steven Englehardt and Arvind Narayanan, "Online tracking: A 1-million-site measurement and analysis," CCS '16: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, https://dl.acm.org/doi/abs/10.1145/2976749.2978313 (October 24, 2016).

[30] Opening Schneier Report ¶ 350 (citing GOOG-CABR-00501220).

Brown v. Google

be joined with a user's signed-in data."[31] Indeed, after a ████████████████████

██

██

██[33]

40.   My review of the documents produced in this case confirms that private browsing information is readily linkable to users and their devices.

41.   In internal Google documents, Google employees wrote that "it is possible for Google to join regular and Incognito sessions,"[34] since Google "log[s] all user activities in incognito mode server-side, and that is more or less linkable to users signed-in data,"[35] Another Google document noted that "There is no join happening between Gaia [Google account identifier referring to a signed-in user] and Zwieback [cookie assigned to any visitor to a Google property or its subsidiaries] but it is theoretically possible via the IP (which is stored with the Zwieback) if the user IP is static."[36] And in an April 2019 email discussing public communication about Incognito mode, a Google product manager wrote, "just keep in mind that we don't actually delete any data and it is saved, just to a pseudonymous ID. The challenge is that we never actually join this data to signed in data, but, in theory, it's possible...."[37] More recently, in a February 2020 comment to an internal Google document, a Google engineer remarked that "IANAL [I am not a lawyer], but from a legal perspective, we would never sa[y] that Google doesn't know who you are while you're Incognito."[38]

42.   Google employees have also specifically noted the joinability risk posed by Google's storage of IP address information. "IP address can be very precise—equivalent to GPS for all intents and purposes, depending on the scenario."[39] Another Google employee likewise explained that "IP address is a viable tracking vector and as such poses a risk to the privacy of users browsing the web."[40] ████████████████████████████████

██

---

[31] Opening Schneier Report ¶ 205 (citing GOOG-BRWN-00386570; GOOG-BRWN-00613801; GOOG-BRWN-00386402; GOOG-CABR-00799341).

[32] GOOG-BRWN-00391406 at -06.

[33] GOOG-BRWN-00184228.

[34] GOOG-BRWN-00705010.

[35] GOOG-BRWN-00701189, GOOG-CABR-00358713.

[36] GOOG-BRWN-00386402.

[37] GOOG-CABR-05270014, cited in Mardini Tr. 346-347.

[38] GOOG-CABR-04780837.R at -40.R.

[39] GOOG-BRWN-00222008.

[40] GOOG-CABR-05250500.

Brown v. Google

███████████████████████████"[41] Consequently, "IP can be used to join the authenticated and incognito sessions."[42]

43.   During his deposition, Google engineer Michael Kleber described the IP address as "one [...] tool that could be used to recognize the same browser as it visits different websites."[43] And Brian Rakowski, deemed the "Father" of Incognito, has acknowledged that the IP address can be used for fingerprinting.[44]

44.   The combination of IP address and user agent information can be used to join a user's private browsing information with the user's other browsing activities. Internal Google documents state that "for some populations, the User-Agent and IP address will often uniquely identify a particular user's browser."[45] "'Combining IP with other data' can be trivial when it comes to things like your user agent."[46] Google engineer Michael Kleber even described the "user-agent string" as "a worst-case scenario" if "your hope is limiting the amount of, like, finger-printable information that might be learned about a web browser."[47]

45.   Because of the abundance of information that Google collects from users during their private browsing, Google employees recognize that this information "could be joinable on a technical level" "between Incognito sessions"[48] and that "Incognito activity" is "easily joinable."[49] For example, Zwieback is Google's "system for uniquely identifying non-logged in users (browsers),"[50] and "The idea that users behind Zwieback UID is not identifiable if one were to use all of the data we have available is laughable."[51]

██
██
██
██
██
"[53]

---

[41] GOOG-CABR-04417613 at-16.

[42] GOOG-BRWN-00157001.

[43] Kleber January 14, 2022 Tr. 74:17-75:8.

[44] Rakowski Tr. 50:16-18.

[45] GOOG-CABR-04006287 at -88.

[46] GOOG-BRWN-00157001 at -01.

[47] Kleber January 14, 2022 Tr. 161:3-13.

[48] GOOG-CABR-00799341.

[49] GOOG-BRWN-00571598 at -99.

[50] GOOG-CABR-00891788 at -89.

[51] GOOG-BRWN-00433503.

[52] GOOG-CABR-05148261 at -73 (emphasis in original).

[53] GOOG-CABR-05888096 at -104.

Brown v. Google

46.   Another example of identifiers that can be used for matching are those tied to users' accounts with non-Google websites, such as the Google Analytics User-ID.

47.   As Professor Zervas notes, the Chrome browser does not use the cookies collected during normal browsing when a user begins to use Incognito. In other words, the Incognito window initially looks like a totally new user to Google's Ad stack. But because Google is matching cookies on its side to the Analytics User-ID—that is, a persistent ID for a single user derived from data from one or more periods initiated from one or more devices[54]—Google could easily identify the Incognito window as another "device" belonging to that user. Cross-device tracking via the User-ID would enable Google to link the Incognito data to regular browsing data on the server side.[55]

48.   Professor Zervas only briefly mentions the Analytics User-ID, noting that "Google prohibits Google Analytics customers from using data that could be used to personally identify an individual, or data that permanently identifies a particular device."[56] But Professor Zervas is tellingly silent on whether the User-ID *could* be used for such purposes. That Google purports to "prohibit" such use is a tacit admission of its possibility. In fact, User-ID is tied to an individual's account with a non-Google website; User-ID itself thereby qualifies as personally identifiable information.

49.   Google provides some public information on cross-device tracking, although that information addresses developers of websites that employ Google Analytics rather than users of the Chrome browser. These statements make it clear that Google joins data from different devices. From one: "Cross Device reporting in Analytics takes into account people who visit your website multiple times from different devices. Now, instead of seeing metrics in Analytics that show two separate sessions (e.g., one on desktop and the other on mobile), you'll be able to see when users visited your website from two different devices."[57] From another: "The Cross Device reports help you connect data about devices and activities from different sessions so you can get a better understanding of your users and what they do at each step of the conversion process—from initial contact to long-term retention."[58] They do not go into details about how this works, but the mere fact that it exists and works, in my opinion, proves that Incognito browsing can be cross-targeted as well.

50.   This ability to cross-target is not discussed widely. ██████████████████
██

---

[54] Google, "About the User-ID feature," *Analytics Help*, https://support.google.com/analytics/answer/3123662 (accessed May 2, 2022).

[55] Google, "User-ID and Cross Device," *Analytics Help*, https://support.google.com/analytics/topic/6009743?hl=en&ref_topic=1007027 (accessed May 2, 2022).

[56] Zervas Report ¶ 92.

[57] Jesse Savage, "Better understand and reach your customers with new Cross Device capabilities in Google Analytics," *Google Marketing Platform*, https://www.blog.google/products/marketingplatform/360/cross-device-capabilities (July 11, 2018).

[58] Google, "About the Cross Device reports," *Analytics Help*, https://support.google.com/analytics/answer/3234673 (accessed May 2, 2022).

Brown v. Google

51.   Another example of such an identifier is the PPID, or publisher-provided ID, which is an identifier tied to a user's account with a non-Google website that uses Google Ad Manager.[60] PPIDs can be "mapped" to other Google identifiers, such as "Biscotti" identifiers.[61] Professor Zervas did not mention PPIDs at all in his report.

52.   Even Professor Zervas appears to agree that identifiers tied to users' accounts with non-Google websites (e.g., PPID and Analytics User-ID), can be used to join private browsing information with users and devices. He carves out from his opinion a scenario in which the user "sign[s] into the website during the Private Browsing Session."[62]

53.   Based on my experience, and consistent with the many internal Google documents I have reviewed that were apparently not considered by Professor Zervas, it is possible for Google to join a user's private browsing information with the user's device and/or Google account. This is a common issue, with Google able to accomplish this systematically across enormous data sets.

> **3.   Professor Zervas failed to demonstrate that the average Internet user is either aware of or knows they should use the "other settings and available features" that he discusses for private browsing; his opinions in this respect are contrary to my experience and understanding.**

54.   Professor Zervas states that "browsers (including Chrome) have numerous *other* settings and available features that prevent the transmission of certain categories of At-Issue Data,"[63] and goes on to describe several Chrome settings and features, as well as several third-party products and services.

55.   Professor Zervas includes these settings, features, methods, and third-party products:

- Cookie blocking (all or third-party only) through browser settings;
- JavaScript blocking through browser settings, or with Sybu or similar third-party browser extensions;
- Blocking Google Analytics with the Google Analytics Opt-out Add-on extension;

---

[59] GOOG-CABR-04760571

[60] Berntson June 16, 2021 Tr. 86:7-9.

[61] GOOG-BRWN-00027305 at -06.

[62] Zervas Report ¶ 82.

[63] Zervas Report ¶ 9.

Brown v. Google

- Blocking ads and other content with uBlock Origin and similar third-party extensions; and
- Masking IP addresses with a third-party VPN service.

56.   While Professor Zervas presents these settings and features as means by which users can limit Google's data collection while users are browsing privately, he presents no evidence suggesting that any significant number of users have ever employed any of these settings or features while browsing privately.

57.   I also have reviewed Google's survey report submitted by Professor On Amir on April 15, 2022, who likewise did not seek any information regarding usage of these settings and features.

58.   Professor Zervas's failure to provide any quantitative support for his opinions regarding private browsing is especially notable given that he had access to Google systems and employees. If Google systems and employees had offered evidence of any substantial use of these settings and features by users while browsing privately, I would expect that Professor Zervas would have supported his opinion with that evidence. The absence of any such in-house evidence suggests there is none.

59.   Based on my many years of evaluating data privacy and various privacy-enhancing browser settings and features, and having considered the specific settings and features identified by Professor Zervas, I expect that throughout the class period there was minimal if any usage of these settings and features by users while browsing privately. Many studies have demonstrated that, in general, users tend to keep default privacy settings.[64] As explained in one recent article, "Default settings have a powerful effect on people, even if you have the option to change them at any time."[65] That article quotes the vice president of Advocacy for Mozilla, who explained: "At

---

[64] Michael J. Kasdan, "Is Facebook Killing Privacy Softly? The Impact of Facebook's Default Privacy Settings on Online Privacy," *Ledger,* https://jipel.law.nyu.edu/ledger-vol-2-no-2-6-kasdan/ (April 20, 2011).

Michelle Madejski, Maritza Johnson, and Steven M. Bellovin, "The Failure of Online Social Network Privacy Settings," *Columbia University Computer Science Technical Reports,* CUCS-010-11, https://academiccommons.columbia.edu/doi/10.7916/D8NG4ZJ1 (July 8, 2011).

Markus Tschersich and R. Botha, "Understanding the Impact of Default Privacy Settings on Self-Disclosure in Social Network Services Building a Conceptual Model and Measurement Instrument Completed Research Paper," *Semantic Scholar,* https://www.semanticscholar.org/paper/Understanding-the-Impact-of-Default-Privacy-on-in-a-Tschersich-Botha/b68819dc89c150f3d7795aa9b510994cca0de214?p2df (2013). "Several possible reasons for not changing the default settings exist: cognitive and physical laziness; perceiving default as correct, perceiving endorsement from the provider; using the default as a justification for choice, lacking transparency of implication, or lacking skill."

Jason Watson, Heather Richter Lipford, and Andrew Brenner, "Mapping User Preference to Privacy Default Settings," *ACM Transactions on Computer-Human Interaction,* https://www.researchgate.net/publication/283478419_Mapping_User_Preference_to_Privacy_Default_Settings (November 2015). "Managing privacy online can be complex and often users do not change defaults or use granular privacy settings."

[65] Alfred Ng, "Default settings for privacy—we need to talk," CNET, https://www.cnet.com/tech/tech-industry/default-settings-for-privacy-we-need-to-talk/ (December 21, 2019). "[S]tudies have found that organ donation increases in countries where it's the default option. In countries where people must sign up to donate their organs, there's a much lower rate. The same applies to privacy settings, researchers have found in several studies."

Brown v. Google

the baseline, we don't think that people should have to jump through hoops and navigate confusing menus to protect their privacy."

60.   To use any of the settings and features identified by Professor Zervas, a user must first be aware of them. However, none of these settings or features are identified on the Incognito Splash Screen, nor does Professor Zervas identify any widespread effort by Google to make users aware of them. To the contrary, Google's own documents recognize that such settings can be "too hard to find and understand" and "hidden."[66]

61.   Even for those users who become aware of one or more of these settings and features, the next question is whether they would know to *employ* them while browsing privately. Here, again, there are no disclosures to users that would notify them of Google's data collection, and therefore no reason for users to believe that they needed to employ these settings and features.

62.   Professor Zervas never addresses these core problems, which are caused by Google's own misleading disclosures. Google's disclosures regarding private browsing mode, including Chrome Incognito mode, create a false sense of security. (I discuss this at length in Section VI of my opening report.) Google in no way notified users that they should seek out or learn to use any other feature or control that would serve the purpose purportedly accomplished with Incognito mode.

63.   Although cookie blocking through browser settings impacts data transmissions to Google, Google's characterization of Incognito as a "private browsing" mode creates the impression (and therefore would lead a reasonable user to assume, consistent with the testimony by Plaintiffs) that it would not be necessary, especially in the absence of a visible control for cookie blocking on the Incognito Splash Screen. A toggle to enable third-party cookie blocking was only added to the Incognito Splash Screen after the initiation of this action, and this toggle still does not disclose that Google cookies can be "first-party" even on non-Google websites.[67]

64.   Although JavaScript blocking through browser settings impacts data transmissions to Google, Google's characterization of Incognito as a "private browsing" mode would lead a reasonable user to assume that it would not be necessary, especially in the absence of a visible control for JavaScript blocking on the Incognito Splash Screen. In Chrome, controls for JavaScript blocking appear several steps into the Settings menu (Settings → Privacy and Security → Site Settings → JavaScript). Technically unsophisticated users could not be expected to anticipate the need to drill several levels down into their browser settings to achieve truly "private browsing." This is an example of a "dark pattern" that I discuss in my opening report.[68]

65.   Although JavaScript is well-known for its vulnerability to attack,[69] it is a fundamental component of most modern websites. Even if a user succeeded in locating the Chrome browser's

---

[66] GOOG-CABR-00413949 at -76.

[67] Abdel Karim Mardini, "More intuitive privacy and security controls in Chrome," *The Keyword*, https://blog.google/products/chrome/more-intuitive-privacy-and-security-controls-chrome (May 18, 2020).

[68] Opening Schneier Report ¶¶ 138-9.

[69] Michael Hollander, "Most common security vulnerabilities using JavaScript," *Secure Coding*, https://www.securecoding.com/blog/most-common-security-vulnerabilities-using-javascript (August 24, 2020).

Brown v. Google

controls for JavaScript blocking, and even though disabling JavaScript altogether might reduce the likelihood that a user might unwittingly download malware,[70] doing so would also render many websites' functionality significantly degraded, a fact Professor Zervas acknowledges.[71] (The Electronic Frontier Foundation agrees: "Disabling JavaScript breaks a staggering amount of websites, and limits the functionality of many more."[72])

66.   Furthermore, blocking JavaScript would not prevent Google from collecting users' private browsing information, including by way of "tracking pixels." Website developers can add to their page a 1-pixel by 1-pixel colorless image that is hosted by another site, such as Google, that provides analytics services. Effectively, the invisible pixel tells the browser to retrieve an "image" for the page from the analytics site. For example, imagine a scenario where Walmart.com wants to display Google Ads to users who look at certain products. When a user's browser loads the Walmart.com page (whether in Incognito mode or not), code embedded in the page directs the browser to load an "image" from Google. The browser then associates the pixel with another Google cookie in its cache (a cookie deposited previously, probably by another site). From this request, Google now recognizes the user and remembers that they were shopping for (say) a toaster on Walmart.com. When this user then visits other sites featuring Google Ads, Google Ads can target them with Walmart's toaster ads, even if the user is on a different website and even after they have purchased a toaster.

67.   This is illustrated in the following diagram:
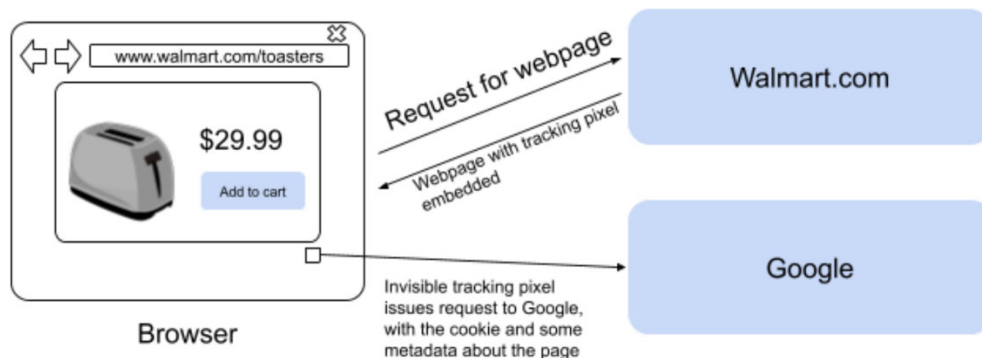
68.   Professor Zervas does not assess Google tracking pixels, let alone their implication for data collection and joinability.

Catherine Graham, "Computer scientist identifies JavaScript vulnerability in thousands of websites," Johns Hopkins University, https://hub.jhu.edu/2022/03/14/computer-scientist-identifies-javascript-vulnerability (March 14, 2022).

[70] Catalin Cimpanu, "Malware found in npm package with millions of weekly downloads," *The Record*, https://therecord media/malware-found-in-npm-package-with-millions-of-weekly-downloads (October 23, 2021).

[71] Zervas Report ¶ 104.

[72] Electronic Frontier Foundation (2020), "How do trackers work?" *Cover Your Tracks*, https://coveryourtracks.eff.org/learn.

Brown v. Google

69.   Professor Zervas discusses several browser extensions that might enhance users' privacy as they browse the web. But as he elsewhere concedes, Incognito mode and Microsoft Edge private browsing automatically disable all extensions.[73]

70.   Although the Google Analytics Opt-out Add-on extension reportedly impacts data transmissions to Google, [74] Google's characterization of Incognito as a "private browsing" mode indicates (and would lead a reasonable user to assume) that it would not be necessary, especially in the absence of a visible control for analytics blocking on the Incognito Splash Screen. Further, the extension would be automatically disabled when a user begins to browse in Incognito mode.

71.   Professor Zervas calls attention to a document outlining policy requirements for site developers using Advertising Features in Google Analytics, in which Google recommends that they "point users to Google Analytics' currently available opt-outs for the web."[75] Those "currently available opt-outs" consist of a single product that is not even named, only linked to from the phrase "currently available opt-outs." Developers are only "encouraged," not "required" to notify users of its availability; websites that link to the app often do so within their privacy policy or cookie policy, ensuring that few visitors will ever see it.[76] Among those visitors who become aware of the extension's existence, only those using a desktop or laptop device will be able to install it, since there is no Android version.

72.   On the Google website, information about the Google Analytics Opt-out Add-on browser extension is found in the "Analytics Help" section, which is addressed to Google Analytics customers, rather than users of the browser.[77] A search for the phrase "analytics opt out" in either Google Chrome Help, or on the Chrome Support section of the Google website, yields no information on the extension, only a single mention of it in a discussion forum.[78] A search for the same phrase on the entire Google site yields links to the app's Chrome Web Store pages in a variety of languages, and some discussion about it by users, but no press releases announcing its availability, and no Google-authored pages recommending it to users who wish to opt out of analytics tracking.

---

[73] Brave, "How to enable extensions in Incognito?" https://brave.com/learn/enable-extensions-in-incognito (November 5, 2020); Zervas Report ¶ 48

[74] Google, "Google Analytics Opt-out Browser Add-on," https://tools.google.com/dlpage/gaoptout (accessed April 28, 2022).

[75] Zervas Report ¶ 93, citing to Google, "Policy requirements for Google Analytics Advertising features," *Analytics Help,* https://support.google.com/analytics/answer/2700409 (last updated April 27, 2022).

[76] See, e.g., Highlands Community Learning Center (August 24, 2022), "Privacy policy," https://hclc.us/privacy-policy; JFE Steel Corporation, "Cookie policy," https://www.jfe-steel.co.jp/en/cookie.html (accessed April 29, 2022).

[77] Google, "Google Analytics opt-out browser add-on," *Analytics Help,* https://support.google.com/analytics/answer/181881 (accessed April 28, 2022).

[78] Google Chrome Help, "Search results for analytics opt out," https://support.google.com/chrome/search?q=%22analytics+opt+out%22 (accessed April 28, 2022).

Google Search, "Search results for analytics opt out site google chrome," https://www.google.com/search?q="analytics+opt+out"+site%3Ahttps%3A%2F%2Fsupport.google.com%2Fchrome (accessed April 28, 2022).

Brown v. Google

73.   The page for the extension in the Chrome Web Store notes that it is "available on Chrome";[79] users of other browsers are led to the Chrome browser download page. In contrast, the page for the same extension in Google Tools notes that it is "available for Google Chrome, Mozilla Firefox, Apple Safari and Microsoft Edge."[80] The Chrome Web Store page indicates that the current version is Version 1.1, updated January 26, 2021; however, the earliest review is dated November 25, 2011, and many subsequent reviewers report problems with the extension.[81] This suggests that over the course of a decade in which Google updated the Chrome browser approximately eighty times,[82] Google expended little effort to update and refine this tool. As one reviewer noted, "It's very fishy that you have to install *an add-on* for this opt-out feature to work to begin with, no matter if it officially comes from Google themselves. This should rather be set in the settings on the Google website—as you would expect."[83]

74.   Even though the Google Analytics Opt-out Add-on extension was developed by Google, Professor Zervas's report may be the only instance in which someone speaking on behalf of Google has recommended it to users of the Chrome browser, let alone users of Chrome's Incognito mode. Users not privy to Professor Zervas's report could not be expected to anticipate the need to install a special browser extension while using Incognito mode.

75.   Even to the extent uBlock Origin and similar ad blockers impact data transmissions to Google, Google's characterization of Incognito as a "private browsing" mode would lead a reasonable user to assume that it would not be necessary, especially in the absence of any explicit recommendation by Google to users who have expressed their desire for privacy by choosing Incognito mode. Further, even if a user installed these extensions, they would be automatically disabled when the user begins browsing in Incognito mode.

76.   As with the Google Analytics Opt-out Add-on extension, a search of the Google website for "uBlock Origin" yields no press releases, no blog posts, and no official recommendations of this third-party product. Chrome users not privy to Professor Zervas's report could not be expected to anticipate the need to install a third-party ad blocker while using Incognito mode.

---

[79] Google, "Google Analytics Opt-out Add-on (by Google)," Chrome Web Store, https://chrome.google.com/webstore/detail/google-analytics-opt-out/fllaojicojecljbmefodhfapmkghcbnh (accessed May 3, 2022).

[80] Google, "Google Analytics Opt-out Add-on," Google Tools, https://tools.google.com/dlpage/gaoptout (accessed May 3, 2022).

[81] Google, "Google Analytics Opt-out Add-on (by Google)," Chrome Web Store, https://chrome.google.com/webstore/detail/google-analytics-opt-out/fllaojicojecljbmefodhfapmkghcbnh (accessed May 3, 2022).

[82] Wikipedia, "Google Chrome version history," https://en.wikipedia.org/wiki/Google_Chrome_version_history (last edited April 29, 2022).

[83] Rafael Cieslik, "Review of Google Analytics Opt-out Add-on (by Google)," https://chrome.google.com/webstore/detail/google-analytics-opt-out/fllaojicojecljbmefodhfapmkghcbnh?hl=en (February 19, 2015).

Brown v. Google

77.   Moreover, the use of extensions like the ones touted by Professor Zervas can actually make a user's browser fingerprint even more likely to be unique, potentially further undermining that user's privacy.[84]

78.   As for VPNs, even to the extent they are able to mask users' IP addresses, this is an additional piece of third-party software that users need to understand and configure, and a service to which they must subscribe. VPN subscriptions cost $10–$15/month on average, a significant deterrent to widespread adoption and beyond the price sensitivity or financial reach of many users.[85]

79.   Even to the extent that the "other settings and available features" outlined by Professor Zervas are capable of affecting data transmissions to Google, Google's inaccurate disclosures and assurances regarding private browsing would lead reasonable users to conclude that additional privacy-protecting measures would be unnecessary during private browsing.

80.   None of the technical measures outlined by Professor Zervas are even mentioned in Incognito mode documentation,[86] let alone suggested to users by Google's representatives as appropriate supplements to Incognito mode. Although Professor Zervas frames these technical measures as a means of minimizing the transmission of browsing information, Google has never officially suggested that users deploy any additional settings, features, or third-party products and services in order to minimize the transmission of private browsing information.

81.   Nor is there any reason for Internet users to know about or learn to use those technical measures because Google has represented private browsing mode itself as a control that prevents Google from collecting users' browsing data. Recall the assurances publicly offered by Google's former CEO, Eric Schmidt, regarding the level of privacy protection afforded by Incognito mode: "Google is so concerned about privacy that you could in fact, if you're using Chrome for example, you can browse in what is called 'incognito mode' where no one sees anything about you."[87] As I noted in my opening report, a Chrome user would reasonably conclude that "no one" would include Google.[88]

82.   Even if a single user enabled cookie and JavaScript blocking, installed the Google Analytics Opt-out Add-on and uBlock Origin extensions, and subscribed to a VPN, that would

---

[84] Sven Taylor (23 Feb 2022), "Browser fingerprinting protection: How to stay private," *Restore Privacy*, https://restoreprivacy.com/browser-fingerprinting.

[85] Sarah Shelton, Bryce Colburn and Jeff Kinnery, "Best VPNs of 2022," *U.S. News and World Report,* https://www.usnews.com/360-reviews/privacy/vpn. (April 21, 2022)

[86] Google, "Browse in private," https://support.google.com/chrome/answer/95464 (accessed April 28, 2022).

Google, "How private browsing works in Chrome," https://support.google.com/chrome/answer/7440301 (accessed April 28, 2022).

Google, "How Chrome Incognito keeps your browsing private," https://support.google.com/chrome/answer/9845881 (accessed April 28, 2022).

[87] Nicole Sawyer (23 Sep 2014), "Google's Eric Schmidt calls Julian Assange 'paranoid' and says Tim Cook is wrong," ABC News, https://abcnews.go.com/Business/googles-eric-schmidt-calls-julian-assange-paranoid-tim/story?id=25679642.

[88] Opening Schneier Report ¶ 286.

not relieve Google of the responsibility of clarifying to Chrome users that their browsing information would continue to be collected and stored while using Incognito mode.

4. Professor Zervas failed to consider Google's financial incentives to make it difficult for users to escape Google's tracking beacons.

83.   Professor Zervas tellingly does not suggest that private browsing users are likely to employ any of the settings or features discussed above, let alone that Google recommends that private browsing users do so, since they do not. Google is financially incentivized to continue misrepresenting private browsing as a control that stops its collection of data. This way, privacy-conscious users will continue to use Incognito mode without trying to figure out how to use any other settings or features that might succeed in blocking Google's tracking beacons.

84.   ███[89]

85.   Google profits greatly from the collection and use of browsing information, including private browsing information; all of this activity contributes to Google's "proprietary user data"—that is, its store of information about individuals. It is in Google's financial interest to collect as much browsing information as possible. Users who seek to minimize Google's collection of information about them undermine the company's above-stated goal of comprehensively tracking, analyzing, profiling, and targeting them for Google's own benefit. Therefore, Google is incentivized to make it difficult for users to conclusively stop the transmission of browsing information to Google. ████████████████████████████████ ████████████████"[90]

86.   Google's obscure placement of information about the Google Analytics Opt-out Add-on extension is a case in point. Although it is likely that many Chrome users would appreciate the functionality that the extension claims to provide, describing it only on the Analytics Help site, and nowhere on the Google Chrome Help site, would tend to make that information available primarily to Google Analytics customers—that is, website owners and computer programmers—rather than users of the browser. Obscurity is also effected by burying the name of the extension inside a link on a developer help page, suggesting rather than requiring that developers include that link in their site's Privacy Policy, expending precious little effort on improving the product, and relegating its functionality to an extension rather than incorporating it into the Chrome browser.

87.   Professor Zervas also fails to account for the manner in which Google is distinguished from other browser developers by the variety and ubiquity of its products.

---

[89] GOOG-CABR-04760571, p. 1.

[90] GOOG-CABR-04154452.

88.   He compares the functionality and disclosures of various Private Browsing modes, and concludes that they "work as described by Google and other companies by concealing users' browsing activity from other people who may use the same device, and by ensuring that cookie values generated during the Private Browsing Sessions cannot be used to provide a link to the user's browsing activity in Regular Mode."[91]

89.   Professor Zervas does not and can not conclude that Google had notified Google account holders that Google would continue to collect information pertaining to their private browsing for the benefit of the advertising arm of their business, because no such notification was ever offered.

90.   Professor Zervas refers to Hotjar, Mixpanel, Matomo, Piwik PRO, and Adobe Analytics, as examples of services similar to Google Analytics that also rely on the use of cookies.[92] To my knowledge, only Google simultaneously offers a search engine, web browser, and navigation-equipped smartphone operating system that monitors individual users' behavior, and aggregates user data to enhance its advertising and analytics businesses.

91.   Google is also distinguished from other services by the number of cookies it deposits on users' devices, and its ability to correlate data from a user's various devices.

> **5.   Professor Zervas improperly seeks to divorce the terms "Private" and "Incognito" from their context and reasonable understandings, ignoring the documents produced and cited by Google.**

92.   I disagree with Professor Zervas' assertion that private browsing modes, including Chrome Incognito, "work as described in public documentation."[93] Neither internal Google documents and statements by Google employees, nor public documents, support Professor Zervas' assertion.

93.   As I noted in my opening report, when attaching labels like "private" or "incognito" to products, software developers must assume that user expectations will include the broadest scope of such words.[94] If one chooses the term "private" or "privacy" to describe a benefit of a product, one must expect that users will interpret those words to include "freedom from attention" by those one can see, and by those one cannot see.[95]

94.   Google's internal documents support my opinion and undermine Professor Zervas' claim that these products "work as described." As one example, a May 2015 internal Google spreadsheet titled "Top 10 – Identify writing mistakes that are easy to avoid" defines "privacy" as "what you share or don't share with other users; what you *store or don't store with Google*. What's important here is user control."[96] This definition of "privacy" supports my opinion that a

---

[91] Zervas Report ¶ 80.

[92] Zervas Report ¶ 87.

[93] Zervas Report ¶ 5.

[94] Schneier Opening Report ¶ 26.

[95] Schneier Opening Report ¶ 24, citing to *Oxford English Dictionary Online*, "Private" (accessed February 28, 2022).

[96] GOOG-CABR-05836882, Tab 1, Row 19 [emphasis added].

user would reasonably understand the Splash Screen's promise that "Now you can browse privately" to mean "'freedom from unwelcome observation,' including observation by Google"[97] – and in turn undermines Professor Zervas' assertion. In an internal email discussion from February 2017, a Google privacy engineer noted that this provision within the Splash Screen "comes across as an implicit verbal promise from Google."[98] This is also consistent with my opinions and undermines Professor Zervas' assertion.

95.   Professor Zervas ignores the testimony by Google engineer Brian Rakowski, who testified that he would not describe Incognito as a "private browsing mode" even though that is how Google describes it publicly.[99] Mr. Rakowski further testified that the name "Incognito," the "Spy Guy" icon, and the catchphrase "Go Incognito" were chosen by marketing department staff because they "had a bit of fun to them," "a bit of personality," and, hopefully, "would help users understand what the mode was for."[100] But that's not what happened.

96.   Repeatedly throughout Google Chrome's fourteen-year history, Google staffers have acknowledged that user misconceptions arise from Google's visual branding for Incognito and its characterization of Incognito mode as a way to browse "privately";

[103]

97.   Many more statements to this effect by Google staffers directly involved in the development of Incognito mode can be found in Sections 11 and 12 of my opening report. Professor Zervas fails to acknowledge or address any of these statements.

98.   Professor Zervas also ignores how, throughout the history of Google Chrome's Incognito mode, Google staffers lobbied to change the feature's name and iconography so that it no longer creates user misconceptions that put users' privacy at risk.[104] None has ever been implemented,

---

[97] Schneier Opening Report ¶ 301.

[98] GOOG-CABR-00354430 at -33.

[99] Schneier Opening Report ¶ 303, citing to Rakowski Tr. 83:16-22

[100] Schneier Opening Report ¶ 273, citing to Rakowski Tr. 24:9-26:2.

[101] Schneier Opening Report ¶ 303, citing to GOOG-BRWN-00047390.

[102] GOOG-BRWN-00812091.

[103] GOOG-BRWN-00390418.

[104]

Brown v. Google

and Google has since applied the term "Incognito" to various features in its other products, including Google Maps[105] and the now-defunct messaging app Allo.[106]

99.

██

100.   As summarized by another Google engineer: "This isn't just marketing, it isn't just a word, this isn't OK. This is a problem of professional ethics and basic honesty, and if we want to call ourselves security engineers and privacy engineers, we need to fix it."[110]

101.   Instead of addressing this evidence, Professor Zervas himself appears to conflate "Google" with "Chrome," lending further support to my opinion that Google's private browsing disclosures are misleading. Referring to Chrome, Professor Zervas notes: "*Google* describes that Incognito Mode in Chrome will not save information like browsing history and cookies after the Incognito session ends." [emphasis added][111] Like Professor Zervas, Google's own employees have conflated "Chrome" with "Google" in their internal discussions.[112]

██

102.   And as explained in my opening report, discussed by the Court in its prior rulings, and ignored by Professor Zervas, the Splash Screen's omission of "Google" from the list of entities to whom "activity might still be visible" also gives rise to a reasonable expectation that Google will not collect private browsing activity. In an April 2016 email, a Chrome team product manager described Chrome Incognito as "basically an ephemeral browsing mode that doesn't leave traces behind on your local device" but that "does not provide anonymity/invisibility

---

[105] Google, "Use Google Maps in Incognito mode," *Google Maps Help*, https://support.google.com/maps/answer/9430563 (accessed May 3, 2022).

[106] Schneier Opening Report ¶ 363.

[107] GOOG-CABR-00084985 at -043.

[108] GOOG-CABR-05270219 at -33 (emphasis in original).

[109] GOOG-BRWN-00042388 at -403.

[110] GOOG-CABR-04971904 at -04.

[111] Zervas Report ¶ 3 (emphasis added).

[112] GOOG-BRWN-00166653 at -32.

[113] Opening Schneier Report ¶ 296.

Brown v. Google

towards any other party (such as the websites you visit, **or Google.**"[114] Unlike this product manager, however, Chrome's Splash Screen omits "Google" from the list of entities to whom browsing activity might be visible, while including "websites you visit."

103.   Professor Zervas does not dispute that Google could have included "Google" on the Splash Screen list, as this Google employee implies, but Google never did that. ███████████
██ [15]

104.   Professor Zervas also ignores statements by Google executives suggesting that Google's continued and broad use of a misleading term to identify "privacy-protecting" features in Google's products arises from top management's commitment not to linguistic accuracy but to consistent branding. ███
███
███
███
███
█████████████████████ "[117]

105.   Professor Zervas himself asserts that "Private Browsing Modes do not and are not designed to provide users complete anonymity or invisibility as they browse the web."[118] He similarly claims that private browsing mode at best "ensure[s] that other people who use the same device won't see the user's activity after the Private Browsing session is closed."[119] In making those assertions, Professor Zervas ignores the "common misconceptions" described by Google employees tied to Google's branding and promises. Based on my experience and the supporting evidence provided in this case, it is clear that Google contributed to common user misconceptions regarding how private browsing mode works and the privacy provided.

106.   Although he purports to offer an opinion regarding "public documentation" concerning private browsing, Professor Zervas tellingly does not cite any public documents to support his assertion that private browsing modes, including Chrome Incognito, function as described. He even ignores the articles that Google identified in this case that, according to Google, "explain[] that Google receives the at-issue data while users are in Incognito mode."[120] The reason Professor Zervas ignores those is likely because none of the articles cited by Google suggest let alone establish that any users were aware of or consented to Google's collection of their private browsing information. None of the articles cited by Google discuss the fact that Google tracking

---

[114] GOOG-BRWN-00390418 at -18 [emphasis added].

[115] GOOG-CABR-05766200.R at -01.R.

[116] Schneier Opening Report ¶ 43, citing to GOOG-BRWN-00696888.

[117] Schneier Opening Report ¶ 364, citing to GOOG-BRWN-00140157, cited in Halavati Tr. 90:21-91:3.

[118] Zervas Report ¶ 7.

[119] Zervas Report ¶ 2.

[120] Google's Supplemental Resp. to Interrogatory No. 40 (identifying "[n]umerous third-party articles").

beacons cause users' browsers to send users' private browsing data to Google during users' visits to non-Google websites while signed out of Google. Indeed, many say absolutely nothing about private browsing at all, while others echo Google's misleading descriptions of Incognito. And certainly none of the articles disclose that Google has since 2017 been using Incognito detection bits, including "is_chrome_incognito," to tag incoming traffic within its logs as "Incognito."[121] Google even concealed these bits even from Plaintiffs' lawyers in this case, resulting in Google being sanctioned for discovery misconduct.

107.   I have reviewed all of these articles, and I provide a brief summary of each in Appendix 2 to this report. Professor Zervas failed to contend with any of these articles.

108.   In terms of public documentation, Professor Zervas also ignores the website policies cited by Google. In its Supplemental Response to Interrogatory No. 40, Google takes the position that "[t]he websites that use Google services are required to disclose their use of those Services." To support this assertion, Google cites various disclosures and privacy policies published by non-Google websites.[122] Professor Zervas tellingly ignores these website privacy policies, likely because they do not support his assertion that private browsing modes function as described, and they do not disclose that Google still collects browsing data in private browsing.

109.   I have reviewed these policies, and they likewise provide no support for Professor Zervas' stated opinions. None disclose that Google tracking beacons will continue to operate notwithstanding the user's choice of a private browsing mode. Indeed, they mention nothing about Incognito or private browsing, let alone disclose that any-third party resource (such as Google) might receive users' private browsing information. Some of the disclosures do mention the website's use of a Google service (like Analytics), but none of them disclose that such Google services will operate and collect information even when the user has elected a private browsing mode.

<div align="center">* * *</div>

110.   Unfortunately, Google has persisted in its use of names, brand elements, and disclosures that betray the trust of users who express their desire for privacy by turning to Incognito and other private browsing modes. The product name "Incognito mode," its brand elements, Google's disclosures about it, and public-facing statements by Google executives are as essential to an analysis of public misconceptions about Incognito mode as is the product's official documentation, along with Google's disclosures about control and private browsing more broadly. As recognized by Google's employees, Google over-promised and under-delivered in a way that put (and continues to put) user privacy at risk.

---

[121] Docket No. 593-3: Order on Plaintiffs' Motion for Sanctions for Discovery Misconduct Redacted Version of Document Sought to Be Sealed.

[122] GOOG-CABR-05876958-67; GOOG-CABR-05877056-220; GOOG-CABR-05877244-324; GOOG-CABR-05877336-402; GOOG-CABR-05877407-92; GOOG-CABR-05877497-510; GOOG-CABR-05877515-45; GOOG-CABR-05877550-66; GOOG-CABR-05877568-676; GOOG-CABR-05877678-812; GOOG-CABR-05877825-64; GOOG-CABR-05877879-94; GOOG-CABR-05877899-975.

Brown v. Google

Respectfully submitted by,

/s/ Bruce Schneier

Date : June 7, 2022

REBUTTAL EXPERT REPORT OF BRUCE SCHNEIER

June 7, 2022

Appendix 1

Exhibits Relied Upon

Cited Bates-stamped Documents

	GOOG-BRWN-00026989 at -92.
	GOOG-BRWN-00027305 at -06.
	GOOG-BRWN-00029326 at -26.
	GOOG-BRWN-00042388 at -403.
	GOOG-BRWN-00047390 at -392.
	GOOG-BRWN-00140157, cited in Halavati Tr. 90:21-91:3
	GOOG-BRWN-00140297
	GOOG-BRWN-00157001 at -01.
	GOOG-BRWN-00157001.
	GOOG-BRWN-00166653 at -32.
	GOOG-BRWN-00184228.
	GOOG-BRWN-00222008.
	GOOG-BRWN-00386402
	GOOG-BRWN-00386402
	GOOG-BRWN-00386570
	GOOG-BRWN-00390418 at -18 [emphasis added].
	GOOG-BRWN-00390418.
	GOOG-BRWN-00391406 at -06.
	GOOG-BRWN-00433503.
	GOOG-BRWN-00477487
	GOOG-BRWN-00477510
	GOOG-BRWN-00554517 at -18.
	GOOG-BRWN-00569625 at -26.
	GOOG-BRWN-00571598 at -99.
	GOOG-BRWN-00613801
	GOOG-BRWN-00696888
	GOOG-BRWN-00701189
	GOOG-BRWN-00705010
	GOOG-BRWN-00812091.
	GOOG-BRWN-00842731 at -35.
	GOOG-BRWN-00848778 at -80.
	GOOG-CABR-00084985 at -043.
	GOOG-CABR-00094550
	GOOG-CABR-00128941
	GOOG-CABR-00354430 at -33.
	GOOG-CABR-00358713
	GOOG-CABR-00413949 at -76.
	GOOG-CABR-00501220
	GOOG-CABR-00799341).
	GOOG-CABR-00799341.
	GOOG-CABR-00891788 at -89.
	GOOG-CABR-04006287 at -87.
	GOOG-CABR-04006287 at -88.
	GOOG-CABR-04006287 at -88.
	GOOG-CABR-04417613 at-16.

	GOOG-CABR-04665638
	GOOG-CABR-04760571
	GOOG-CABR-04760571, p. 1
	GOOG-CABR-04780837.R at -40.R.
	GOOG-CABR-04971904 at -04.
	GOOG-CABR-05148261 at -73 (emphasis in original).
	GOOG-CABR-05250500.
	GOOG-CABR-05270014, cited in Mardini Tr. 346-347
	GOOG-CABR-05270219 at -33 (emphasis in original).
	GOOG-CABR-05766200.R at -01.R,
	GOOG-CABR-05836882, Tab 1, Row 19 [emphasis added].
	GOOG-CABR-05876958
	GOOG-CABR-05876958-67
	GOOG-CABR-05877056-220
	GOOG-CABR-05877174
	GOOG-CABR-05877244-324
	GOOG-CABR-05877336-402
	GOOG-CABR-05877407-92
	GOOG-CABR-05877497-510
	GOOG-CABR-05877515-45
	GOOG-CABR-05877550-66
	GOOG-CABR-05877568-676
	GOOG-CABR-05877678-812
	GOOG-CABR-05877825-64
	GOOG-CABR-05877879-94
	GOOG-CABR-05877899-975
	GOOG-CABR-05888096 at -104.

Public Exhibits

Brave, "How to enable extensions in Incognito" https://brave.com/learn/enable-extensions-in-incognito/ (2020).

Bill Budington, "How do trackers work" https://www.eff.org/deeplinks/2020/11/introducing-cover-your-tracks (November 19, 2020).

Chrome Web Store, "Google Analytics Opt-out Add-on" https://chrome.google.com/webstore/detail/google-analytics-opt-out (2022).

Cieslik (Chrome Web Store), "Cieslik Review of Google Analytics Opt-Out Add-on" https://chrome.google.com/webstore/detail/google-analytics-opt-out (2022).

Catalin Cimpanu, "Malware found in npm package with millions of weekly downloads" https://therecord.media/malware-found-in-npm-package-with-millions-of-weekly-downloads/ (October 23, 2021)

Kendra Clark, "Google Analytics stops logging IP addresses: here's why it's a big deal for marketers" https://www.thedrum.com/news/2022/03/16/google-analytics-nixes-ip-address-logging-new-privacy-play#:~:text=Google%20is%20axing%20Internet%20Protocol,context%20of%20maturing%20privacy%20standards. (March 16, 2022).

Joseph Cox, "Data broker is selling location data of people who visit abortion clinics" https://www.vice.com/en/article/m7vzjb/location-data-abortion-clinics-safegraph-planned-parenthood (May 3, 2022).

Anthony Cuthbertson, "Google Chrome's private incognito mode leaks way more personal data than you might think" https://www.independent.co.uk/tech/google-chrome-incognito-mode-personal-data-private-browser-a8502386.html (August 22, 2018).

Peter Eckersley, "How unique is your web browser" https://coveryourtracks.eff.org/static/browser-uniqueness (2010).

Steven Englehart, "Online Tracking:A 1-million-site Measurement and Analysis" https://www.cs.princeton.edu/~arvindn/publications/OpenWPM_1_million_site_tracking_measurement.pdf (2016).

Corin Faife "ICE uses data brokers to bypass surveillance restrictions" https://www.theverge.com/2022/5/10/23065080/ice-surveillance-dragnet-data-brokers-georgetown-law (May 10, 2022).

Corin Faife, "Democrats say Google must curb location tracking before Roe appeal" https://www.theverge.com/2022/5/24/23140279/democrat-letter-google-location-data-abortion-surveillance-geofence-warrants (May 24, 2022).
Geoffrey A. Fowler, "Your phone could reveal if you've had an abortion" https://www.washingtonpost.com/technology/2022/05/04/abortion-digital-privacy/ (May 4, 2022).

Google Analytics Help, "About the Cross Device reports" https://support.google.com/analytics/answer/3234673?hl=en (2022).

Google Analytics Help, "About the User ID feature" https://support.google.com/analytics/answer/3123669?hl=en (2022).

Google Analytics Help, "Google Analytics opt-out browser add-on" https://support.google.com/analytics/answer/181881?hl=en (2022).

Google Analytics Help, "User-ID and Cross Device" https://support.google.com/analytics/answer/3234673?hl=en (2022).

Google Analytics Support, "Policy requirements for Google Analytics Advertising Features" https://support.google.com/analytics/answer/2700409?hl=en (2022).

Google Chrome Help, "Browse in private" https://support.google.com/chrome/answer/95464 (2022).

Google Chrome Help, "How Chrome Incognito keeps your browsing private" https://support.google.com/chrome/answer/9845881?hl=en (2022).

Google Chrome Help, "How private browsing works in Chrome - Computer" https://support.google.com/chrome/answer/7440301?hl=en&co=GENIE.Platform%3DDesktop (2022).

Google Chrome Help, "Search results for analytics opt out" https://support.google.com/analytics/answer/181881?hl=en (2022).

Google Maps Help, "Use Google Maps in Incognito mode" https://support.google.com/maps/answer/9430563?hl=en&co=GENIE.Platform%3DAndroid (2022).

Google Search, "Search results for analytics opt out site google chrome" https://support.google.com/chrome#topic=9796470 (2022).

Google Tools, "Google Analytics Opt-out Browser Add-on" https://tools.google.com/dlpage/gaoptout (2022).

Catherine Graham, "Computer scientist identifies JavaScript vulnerability in thousands of websites" https://hub.jhu.edu/2022/03/14/computer-scientist-identifies-javascript-vulnerability/ (March 14, 2022).

James Hercher. "Google Analytics To Stop Logging IP Addresses And Sunset Old Versions In Privacy Standards Overhaul" https://www.adexchanger.com/online-advertising/google-analytics-to-stop-logging-ip-addresses-and-sunset-old-versions-in-privacy-standards-overhaul/ (March 16, 2022).

Highlands Community Learning Center, "Privacy policy" https://hclc.us/privacy-policy (2022).

Michael Hollander, "Most common security vulnerabilities using JavaScript" https://www.securecoding.com/blog/most-common-security-vulnerabilities-using-javascript/ August 24, 2020).

JFE Steel Corporation, "Cookie Policy" https://www.jfe-steel.co.jp/en/cookie.html (2022).

Russell Ketchum, " Prepare for the future with Google Analytics 4" https://blog.google/products/marketingplatform/analytics/prepare-for-future-with-google-analytics-4/ (March 16, 2022).

Abdelkarim Mardini, "More intuitive privacy and security controls in Chrome"
https://blog.google/products/chrome/more-intuitive-privacy-and-security-controls-chrome/ (May
19, 2020).

Alfred Ng, "Default settings for privacy—we need to talk," CNET
https://www.cnet.com/tech/tech-industry/default-settings-for-privacy-we-need-to-talk/
(December 21, 2019).

Nick Nikiforakis, "Cookieless monster - Exploring the ecosystem of web-based device
fingerprinting" https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6547132 (2013).

OED, "Private (definition)"
https://www.oxfordlearnersdictionaries.com/us/definition/english/private_1 (2022).

Barbara Ortutay, "Democrats - Google must protect privacy of abortion patients"
https://www.washingtonpost.com/politics/democrats-ask-google-to-protect-abortion-patient-
privacy/2022/05/24/5e7bd54e-db97-11ec-bc35-a91d0a94923b_story.html (May 24, 2022).

Jesse Savage, "Better understand and reach your customers with new Cross Device capabilities
in Google Analytics" https://analytics.googleblog.com/2018/07/cross-device-capabilities-
mktg.html (July 11, 2018).

Nicole Sawyer, "Google's Eric Schmidt calls Julian Assange 'paranoid' and says Tim Cook is
wrong" https://abcnews.go.com/Business/googles-eric-schmidt-calls-julian-assange-paranoid-
tim/story?id=25679642 (September 23, 2014).

Schmidt, "Google data collection" https://digitalcontentnext.org/blog/2018/08/21/google-data-
collection-research/ (August 21, 2018).

Schreiber, "US states could ban people from traveling for abortions, experts warn"
https://www.theguardian.com/world/2022/may/03/us-abortions-travel-wave-of-restrictions)May
3, 2022).

Sarah Shelton, "Best VPNs of 2022" https://www.usnews.com/360-reviews/privacy/vpn (May
23, 2022).

Sven Taylor, " Browser fingerprinting protection" https://restoreprivacy.com/browser-
fingerprinting/ (February 23, 2022).

Weather Channel, "Vendor privacy practices and opt outs" https://weather.com/en-
US/twc/privacy-policy (2022).

Wikipedia, "Google Chrome version history"
https://en.wikipedia.org/wiki/Google_Chrome_version_history (2022).

How to enable extensions in Incognito?

← **See all articles**

Table of contents

Incognito and private browsing

When (and when not) to use Incognito mode

Allowing extensions in Incognito mode

Brave's Private Window with Tor and extensions

Last updated Nov 5, 2020   Tweet this article 🐦

Nearly every browser has a version of Chrome's Incognito mode, designed to keep your browsing history hidden from other users on the same computer. But will your favorite extensions work in Incognito mode?

It is important to note that browsing in Incognito mode will not keep your actions hidden from trackers and ads on the Internet; Incognito mode is no private browser. But if you are using Incognito mode and want to keep your extensions at the same time, we'll show you how in this article.

Brave Talk for meetings!   ✕

third-party trackers and unwanted ads.

Incognito and private browsing

Incognito on browsers like Chrome do little more than prevent the browser from storing your search history on that device. It does nothing about the websites you visit or any trackers on the Internet. As far as the websites you visit are concerned, Incognito mode is the same as normal browsing.

Truly private browsing is something different. A private browser keeps your habits hidden from third-party trackers and websites themselves, helping to keep you safely anonymous on the Internet.

When (and when not) to use Incognito mode

Incognito mode keeps things hidden on the user's side, so browse with Incognito mode when you are trying to hide your history from other users on the same device. Buying a secret birthday gift or planning a surprise holiday? Incognito mode is the way to go. Your browsing history will be deleted when you end the session, and no other users on the same device can see what you did.

If you have genuine concerns about your Internet privacy, don't rely solely on Incognito mode. Only a few browsers have a private browsing mode that actually keeps you hidden from third parties. Brave's Private Window with Tor is one example since it uses the Tor network to relay your connection through three different devices and keep you anonymous

Brave Talk for meetings! ✕

Allowing extensions in Incognito mode

1. Brave

Brave automatically disables extensions in Private browsing mode.

To enable them, you'll need to find Preferences under the Brave menu.

Then select Extensions > Manage Extensions, and find the extension you want to allow.

Click "More Details" under that extension, and you should see an option to "Allow in Private browsing."

You will also see a warning, notifying you that any extension you allow will have the ability to see your activity.

2. Chrome

In Chrome, your extensions as a general rule do not work in Incognito mode. Because extensions are a third-party addition to your browser, and most are tracking your browsing history for better performance, Incognito mode automatically disables them.

Both Brave and Chrome require users to explicitly enable extensions for private windows.

You will need to adjust the settings in your browser.

Open Chrome > Menu > More Tools > Extensions.

Brave Talk for meetings!   ✕

to enable the extension in Incognito mode, then the extension may not work.

3. Firefox

Firefox, just like Chrome and Brave, does not automatically allow your extensions to work in Private Browsing mode (Firefox's version of Incognito).

To give permission for your extensions to work, you'll need to open Firefox.

Select Menu > Add-ons > Extensions > Run in Private Windows > Allow

4. Edge

Microsoft Edge calls Incognito "Private browsing" and requires that you enable extensions to work in private browsing.

To change this feature, you'll need to open Edge, select Menu > Extensions > Installed Extensions.

To turn on Private Browsing for each extension, you'll need to select Details under each extension and choose "Allow in Private".

Turning on an extension to work in private mode does not change the extension itself. If it is insecure, your browsing will be compromised whether you are in Private Browsing mode or not. It is important you know exactly what extensions you have downloaded and given permissions to.

Brave's Private Window with Tor and extensions

Brave Talk for meetings!

✕

normal one, and one that adds the protection of the Tor network to your private browsing window.

Brave's Private Window with Tor routes your connection through three relays in the Tor network. Each step knows only the next step in the chain – the point of origin is kept anonymous, meaning that it is extremely difficult for websites to identify you and track your habits.

With Brave, you get the benefits of Tor plus all the benefits of Brave, along with an extra layer of protection for you in private mode.

Related articles

Brave Talk for meetings!   ✕

What's the best private browser?

Many users rely on private browsers to keep their Internet habits away from prying eyes. But with so many options out there, what's the best private…

Read this article →

What is a no-tracking search engine?

There are a number of search engines that do not track your search history. These no-tracking search engines deliver high-quality results and keep…

Read this article →

Does incognito hide your IP?

What exactly does Incognito mode do? Is it actually more private? Does it hide your IP address? In this short article, we'll discuss incognito windows, IP…

Read this article →

Ready to Brave the new internet?

Brave Talk for meetings!   ✕

Download Brave for Windows 64-bit

Brave Talk for meetings!   ✕

Resources

F.A.Q

Help Center

Community

Status

Transparency Report

Learn

Insights

Privacy Policy

Brave Browser

Website & Email

Publishers & Creators

Advertisers

Product

Brave Release

Brave Beta

Brave Nightly

Company

About

Research

Careers

Brand Assets

Media Kit

In the Press

GitHub

Blog

Tor Onion Address

Social Media

Reddit

Twitter

Facebook

YouTube

Contact

Support

community.brave.com

Advertising

adsales@brave.com

Business

Offices

Brave San Francisco

580 Howard St. Unit 402,
San Francisco, CA 94105

Choose a language

English

Brave Talk for meetings!

✕

Terms of Use | Report a Security Issue

Brave Talk for meetings!

✕

Cover Your Tracks

How do trackers work?
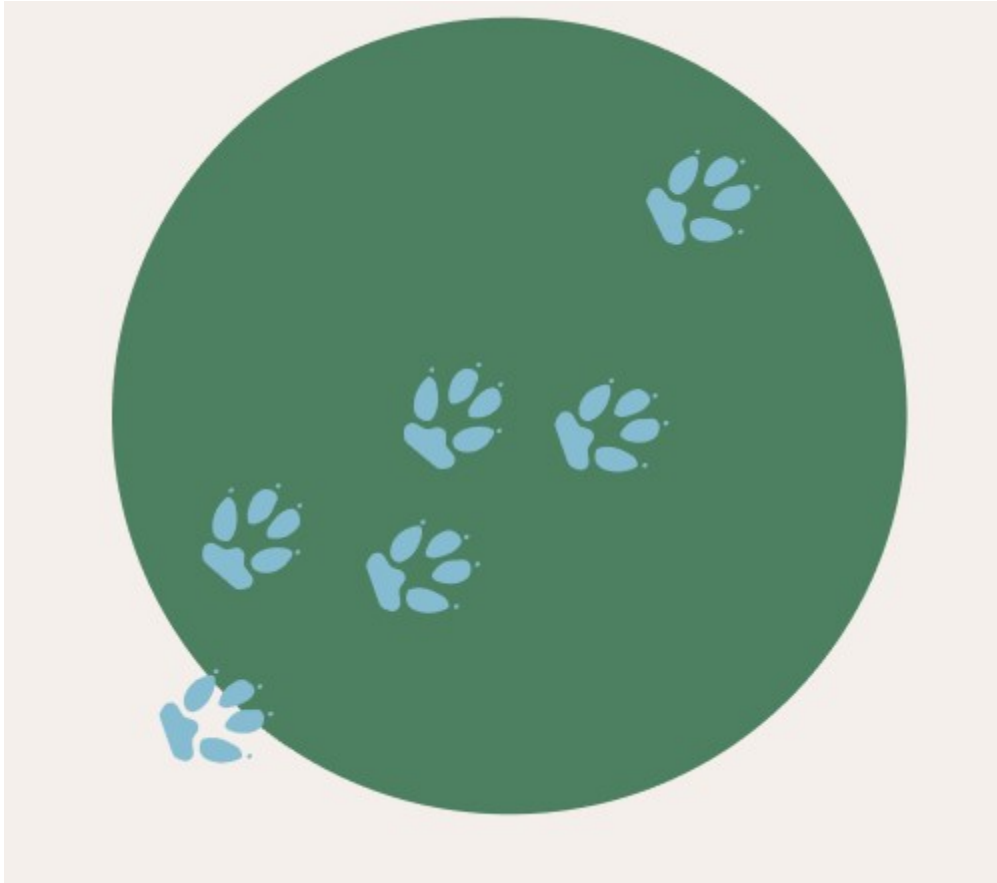
When you visit a website, your browser makes a "request" for that site. In the background, advertising code and invisible trackers on that site might also cause your browser to make dozens or even hundreds of requests to other hidden third parties. Each request contains several pieces of information about your browser and about you, from your time zone to your browser settings to what versions of software you have installed.

Some of this information is passed along by default simply to help you view the page. For example, HTTP headers are essential to most web functionality, and broadcast your device and browser version. But a lot of the information in your browser's requests is also extracted by third-party ad networks, which have sneaky tracking mechanisms embedded across the Internet to gather your information.

At first glance, the data points that third-party trackers collect may seem relatively mundane and disparate. But when compiled together, they can reveal a detailed behavioral profile of your online activity, from political affiliation to education level to income bracket. As long as this trove of data about you is linked back to you, your online activity can be logged. Ad networks primarily rely on two methods to maintain this link: cookie tracking, and browser fingerprinting.

What are cookies?

Cookies are small chunks of information that websites store in your browser. Their main use is to remember helpful things like your account login info, or what items were in your online shopping cart—in other words, they save your place. But they can also be misused to link all your visits, searches, and other activities on a site together. This use of cookies is a privacy violation, and browsers generally allow you to block, limit, or delete cookies.

What is a digital fingerprint?

A digital fingerprint is essentially a list of characteristics that are unique to a single user, their browser, and their particular hardware setup. This includes information the browser needs to send to access websites, like the location of the website the user is requesting. But it also includes a host of seemingly insignificant data (like screen resolution and installed fonts) gathered by tracking scripts. Tracking sites can stitch all the small pieces together to form a unique picture, or "fingerprint," of your device.

What is the difference?

Think of the small tracking devices scientists use to follow animal migration patterns, or a GPS transmitter attached to a car. As long as they're attached to the target animal or vehicle, they are accurate and effective—but they lose all value if they're knocked off or discarded. This is roughly how cookies behave: they track users up until the point a user deletes them.

Fingerprinting uses more permanent identifiers such as hardware specifications and browser settings. This is equivalent to tracking a bird by its song or feather markings, or a car by its license plate, make, model, and color. In other words, metrics that are harder to change and impossible to delete.

Can I do anything about this?!

Completely blocking trackers is difficult, even with a fully-featured tracker blocker. Even so, **we recommend using the tracking protections above**. Privacy protection does not have to be perfect to make a big difference!

There are two main dynamics that make trackers hard to entirely avoid online:

1. **Impact on Usability:** It's unfortunate that enhanced privacy often comes at the expense of functionality. For instance, you may want to disable JavaScript to stop tracking scripts from running. But this will likely make it hard to shop, fill out forms, watch videos, or see interactive web elements. Many pages require disabling your ad blocker to see content, or refuse to load anything unless you use the "official" app.
2. **Identifiable Protections:** Paradoxically, sometimes your protections themselves can become part of your fingerprint. An add-on intended to protect you can even lead to your full identification. Changing your settings and installing protections can lead trackers to be identified. In this case, you become a "mystery user with a very specific combination of privacy protections installed."

In practice, the most realistic protection currently available is the Tor Browser, which has put a lot of effort into reducing browser fingerprintability. For day-to-day use, the best options are to run tools like Privacy Badger or Disconnect that will block some (but unfortunately not all) of the domains that try to perform fingerprinting, and/or to use a tool like NoScript(for Firefox), which greatly reduces the amount of data available to fingerprinters.

Cover Your Tracks' primary goal is to help you determine your own balance between privacy and convenience. By giving you a summary of your overall protection and a list of characteristics that make up your digital fingerprint, you can see exactly how your browser appears to trackers, and how implementing different protection methods changes this visibility. The following suggestions are simple, straightforward protection methods, and are an excellent starting point.
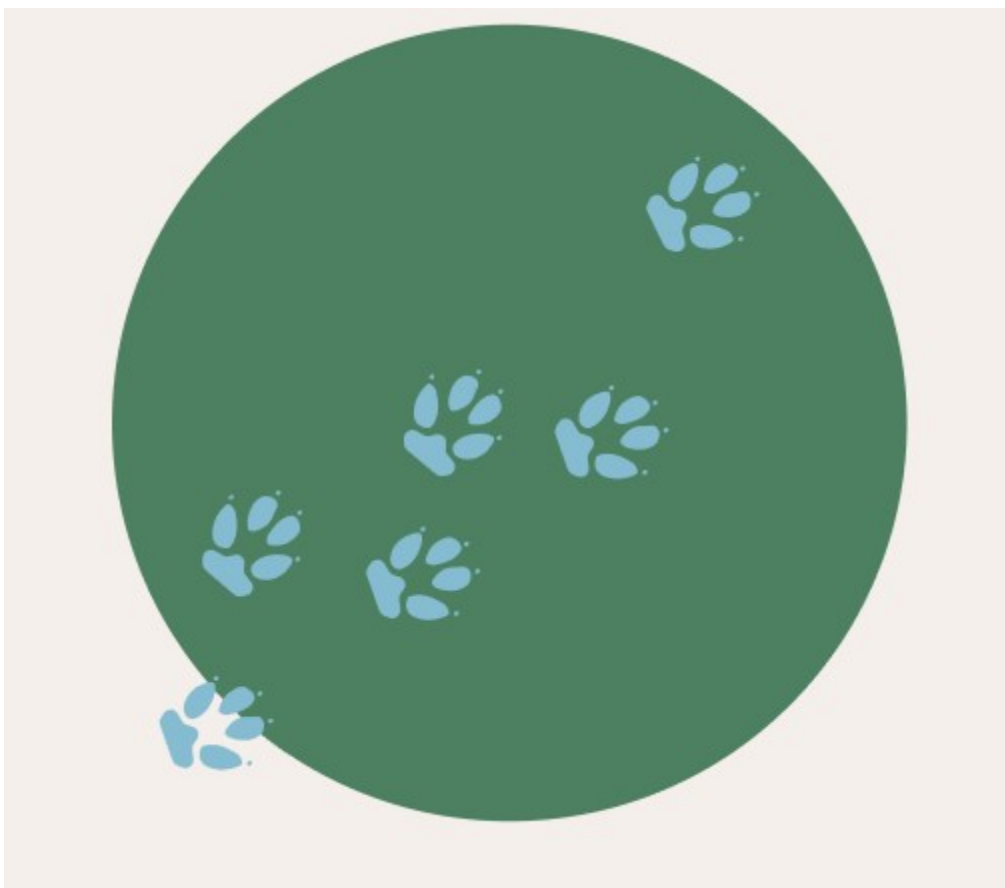
Simple suggestions

Using a Tracker Blocker

Install a tracker blocker and watch your browsing experience get a lot more pleasant

Most tracker blockers cross-reference massive lists of tracking scripts. They then block any attempts to load an ad or other item that matches.

When you block trackers, you prevent tracking companies from reading your browser fingerprint. However, more advanced tracking techniques may still be able to gather information about you.

Disabling Javascript

Most trackers run on JavaScript, and they can't gather much of the information used to determine your browser fingerprint without it. Thus, your browser looks a lot less distinct, and is more protected.

But there is a trade off. Disabling JavaScript breaks a staggering amount of websites, and limits the functionality of many more.

Changing browser settings from defaults

Tracking is so pervasive that all of the major browsers (Chrome, Firefox, and Safari) come with settings that disable certain types of tracking. Turning them on or off is as simple as going into the settings menu and clicking a button.

Disabling tracking scripts in your browser settings is reliably effective, though not as robust as a designated tracker-blocker.

For more info about what settings and protections your browser offers compared to others, check out this article [from Blacklight](#).

Using a fingerprint resistant browser

Some newer browsers were built to thwart fingerprinting, such as Tor Browser and Brave. How they do this varies from browser to browser, but they generally work by making your fingerprint less unique and/or less consistent. This means trackers have a harder time following your usage of the web.

Can my attempts to protect myself backfire? How can attempting to make myself more anonymous actually make me more identifiable?

Each browser metric is highly connected to other metrics in complex ways. This is why we *don't recommend* trying to change a single element of your fingerprint. Striving to get the most common result for any individual metric may seem like a good idea, but it can actually make your browser more identifiable.

Let's look at an example of how these metrics are interconnected:

No matter what browser you're using, they all send information about themselves to servers so that web content loads correctly. This information includes the browser name and version. If you swap out the identifier of the browser you're actually using with one from a more common browser, you may make yourself completely identifiable. How is this possible? If Chrome is a more common browser, how can identifying your browser as Chrome make you more unique?

Because trackers aren't only looking at what browser version you have. In combination with other metrics, your fake Chrome browser may stand out. This is because if you are actually using, say, Safari browser all the other metrics will point to this fact. You will have the only browser out there identifying itself as Chrome but looking like Safari.

Incognito mode

Historically, Private Browsing and Incognito Mode had a single purpose. These modes were intended to prevent traces of sites you visited from being stored on *your machine*. It was not meant to prevent remote sites or trackers from identifying and storing when you visit a site on *their* servers.

If you are using Firefox, using Private Browsing will provide some protections against trackers. Any trackers that are included in the [Disconnect](#) tracking protection list will be blocked. This keeps you safe from *known* trackers. Known fingerprinters and cryptominers which use your browser against you are also blocked. However, this will not prevent a *new* fingerprinter or tracker from identifying your browser and keeping tabs on it. In order to get this extra level of protection, your browser needs to have a fingerprint which is either:

1. so common that a tracker can't tell you apart from the crowd (as in [Tor Browser](#)), or
2. randomized so that a tracker can't tell it's you from one moment to the next (as in Brave browser).

Google's Chrome browser does not provide protection against trackers or fingerprinters in Incognito Mode.

chrome web store   ⚙ Sign in

Home > Extensions > Google Analytics Opt-out Add-on (by Google)

Google Analytics Opt-out Add-on (by Google)   Available on Chrome

◉ Featured

★★★★★ 1,730 | Search Tools | 1,000,000+ users
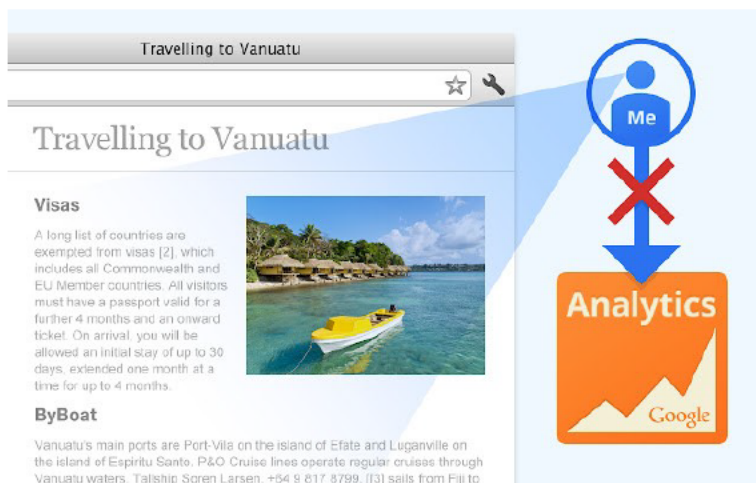
G By Google

Overview   Privacy practices   Reviews   Related

Overview

Tells the Google Analytics JavaScript not to send information to Google Analytics.

To provide website visitors the ability to prevent their data from being collected and used by Google Analytics, we have developed the Google Analytics opt-out Browser extension for the Google Analytics JavaScript (ga.js, analytics.js, dc.js).

If you want to opt-out, download and install the extension for your web browser. In order to function, the opt-out extension must be able to load and execute properly on your browser. Updates to your browser or operating system may affect the functionality of the opt-out extension. More information about managing your extensions for Chrome can be found at https://support.google.com/chrome/answer/187443?hl=en.

By installing this extension, you agree to the Chrome Web Store Terms of Service at https://ssl.gstatic.com/chrome/webstore/intl/en/gallery_tos.html and the Google Analytics Opt-out Browser Add-on Terms of Service at https://tools.google.com/dlpage/gaoptout/intl/en/eula_text.html.

Additional Information

❗ Report abuse

Offered by
ga-extension-publishers

Version
1.1

Updated
January 26, 2021

Size
181KiB

Languages
See all 17

Developer
Contact the developer
Privacy Policy

Related

chrome web store   ⚙ Sign in

Home > Extensions > Google Analytics Opt-out Add-on (by Google)

Google Analytics Opt-out Add-on (by Google)

📍 Featured

★★★★☆ 1,730 | Search Tools | 1,000,000+ users

G By Google

Available on Chrome

Overview   Privacy practices   Reviews   Related

Overview

Tells the Google Analytics JavaScript not to send information to Google Analytics.

To provide website visitors the ability to prevent their data from being collected and used by Google Analytics, we have developed the Google Analytics opt-out Browser extension for the Google Analytics JavaScript (ga.js, analytics.js, dc.js).

If you want to opt-out, download and install the extension for your web browser. In order to function, the opt-out extension must be able to load and execute properly on your browser. Updates to your browser or operating system may affect the functionality of the opt-out extension. More information about managing your extensions for Chrome can be found at https://support.google.com/chrome/answer/187443?hl=en.

By installing this extension, you agree to the Chrome Web Store Terms of Service at https://ssl.gstatic.com/chrome/webstore/intl/en/gallery_tos.html and the Google Analytics Opt-out Browser Add-on Terms of Service at https://tools.google.com/dlpage/gaoptout/intl/en/eula_text.html.

Additional Information

🔴 Report abuse

Offered by
ga-extension-publishers

Version
1.1

Updated
January 26, 2021

Size
181KiB

Languages
See all 17

Developer
Contact the developer
Privacy Policy

Related

chrome web store   ⚙ Sign in

Home > Extensions > Google Analytics Opt-out Add-on (by Google)

Google Analytics Opt-out Add-on (by Google)

Available on Chrome

📍 Featured

★★★★☆ 1,730 | Search Tools | 1,000,000+ users

G By Google

Overview   Privacy practices   Reviews   Related

Overview

Tells the Google Analytics JavaScript not to send information to Google Analytics.

To provide website visitors the ability to prevent their data from being collected and used by Google Analytics, we have developed the Google Analytics opt-out Browser extension for the Google Analytics JavaScript (ga.js, analytics.js, dc.js).

If you want to opt-out, download and install the extension for your web browser. In order to function, the opt-out extension must be able to load and execute properly on your browser. Updates to your browser or operating system may affect the functionality of the opt-out extension. More information about managing your extensions for Chrome can be found at https://support.google.com/chrome/answer/187443?hl=en.

By installing this extension, you agree to the Chrome Web Store Terms of Service at https://ssl.gstatic.com/chrome/webstore/intl/en/gallery_tos.html and the Google Analytics Opt-out Browser Add-on Terms of Service at https://tools.google.com/dlpage/gaoptout/intl/en/eula_text.html.

Additional Information

🔴 Report abuse

Offered by
ga-extension-publishers

Version
1.1

Updated
January 26, 2021

Size
181KiB

Languages
See all 17

Developer
Contact the developer
Privacy Policy

Related

chrome web store

⚙ Sign in

Home > Extensions > Google Analytics Opt-out Add-on (by Google)

Google Analytics Opt-out Add-on (by Google)

📍 Featured

Available on Chrome

★★★★☆ 1,730 | Search Tools | 1,000,000+ users

G By Google

Overview   Privacy practices   Reviews   Related

Overview

Tells the Google Analytics JavaScript not to send information to Google Analytics.

To provide website visitors the ability to prevent their data from being collected and used by Google Analytics, we have developed the Google Analytics opt-out Browser extension for the Google Analytics JavaScript (ga.js, analytics.js, dc.js).

If you want to opt-out, download and install the extension for your web browser. In order to function, the opt-out extension must be able to load and execute properly on your browser. Updates to your browser or operating system may affect the functionality of the opt-out extension. More information about managing your extensions for Chrome can be found at https://support.google.com/chrome/answer/187443?hl=en.

By installing this extension, you agree to the Chrome Web Store Terms of Service at https://ssl.gstatic.com/chrome/webstore/intl/en/gallery_tos.html and the Google Analytics Opt-out Browser Add-on Terms of Service at https://tools.google.com/dlpage/gaoptout/intl/en/eula_text.html.

Additional Information

🛑 Report abuse

Offered by
ga-extension-publishers

Version
1.1

Updated
January 26, 2021

Size
181KiB

Languages
See all 17

Developer
Contact the developer
Privacy Policy

Related

chrome web store   ⚙ Sign in

Google Analytics Opt-out Add-on (by Google)

📍 Featured

Available on Chrome

★★★★☆ 1,730 | Search Tools | 1,000,000+ users

G By Google

Overview   Privacy practices   Reviews   Related

Overview

Tells the Google Analytics JavaScript not to send information to Google Analytics.

To provide website visitors the ability to prevent their data from being collected and used by Google Analytics, we have developed the Google Analytics opt-out Browser extension for the Google Analytics JavaScript (ga.js, analytics.js, dc.js).

If you want to opt-out, download and install the extension for your web browser. In order to function, the opt-out extension must be able to load and execute properly on your browser. Updates to your browser or operating system may affect the functionality of the opt-out extension. More information about managing your extensions for Chrome can be found at https://support.google.com/chrome/answer/187443?hl=en.

By installing this extension, you agree to the Chrome Web Store Terms of Service at https://ssl.gstatic.com/chrome/webstore/intl/en/gallery_tos.html and the Google Analytics Opt-out Browser Add-on Terms of Service at https://tools.google.com/dlpage/gaoptout/intl/en/eula_text.html.

Additional Information

🔴 Report abuse

Offered by
ga-extension-publishers

Version
1.1

Updated
January 26, 2021

Size
181KiB

Languages
See all 17

Developer
Contact the developer
Privacy Policy

Related

chrome web store   ⚙ Sign in

Home > Extensions > Google Analytics Opt-out Add-on (by Google)

Google Analytics Opt-out Add-on (by Google)   Available on Chrome

📍 Featured

★★★★☆ 1,730 | Search Tools | 1,000,000+ users

G By Google

Overview   Privacy practices   Reviews   Related

User Reviews   [Write a review]   English   Helpful

Alpine Observer   Modified Aug 6, 2017   ★★★★★

After several days of using this extension I then recently noticed that Chrome was not connecting to the internet at all, no sites at all. Other browsers were working OK. I spent over an hour troubleshooting, but no joy.

Then, I disabled all extensions, and Chrome starting working again. So I re-enabled all other extensions and Chrome kept on working....until I re-enabled this extension, then it stopped connecting to the internet entirely again!

So now this extension is disabled, and meanwhile Google keep on sucking up all my browsing information and invading my privacy.

I concluded that Google perhaps have ZERO interest in making this an effective extension because it reduces how much of your information and privacy they can steal?

Was this review helpful? ○ Yes   ○ No   Reply | Mark as spam or abuse

> **Hexane Smith**   Feb 2, 2022
>
> Google knows me better than anyone else, better than even I do.
> Look on the bright side - after we die, we can live again once they figure out how to sort all of this information into a coherent being. Which can be advertised to for all eternity! (Seriously, I hope whatever AI takes over they make sure that no semi-eternal synthetic lifeforms are capable of semi-eternal suffering. At least with us meatbags it's limited to 110 years max).
>
> Was this review helpful? ○ Yes   ○ No | Mark as spam or abuse

> **Abinash Senapati**   Sep 14, 2017
>
> Do you have a dynamic ip or just a static one. For static just add filter in google analytics itself and for the dynamic if this extension not working as you have already said then just add a custom filter in google analytics as "user defined-cookie_filter" :)
>
> Was this review helpful? ○ Yes   ○ No | Mark as spam or abuse

Paulie Webster   Modified Oct 7, 2016   ★★★★★

Works perfectly. Lots of bad reviews saying it doesn't work. Not sure why, maybe people think it removes the code from your webpage? That's not how the internet works? This extension tells the analytics code not to fire. I just tested it on my site, and with the extension enabled, Google Analytics Real-Time didn't see my site views or my contact form goal conversions. But when I disabled the extension, Analytics could see me again. As far as I can tell this works perfectly. Thanks!

Was this review helpful? ○ Yes   ○ No   Reply | Mark as spam or abuse

chrome web store   ⚙ Sign in

Home > Extensions > Google Analytics Opt-out Add-on (by Google)

Google Analytics Opt-out Add-on (by Google)

Available on Chrome

◉ Featured

★★★★★ 1,730 | Search Tools | 1,000,000+ users

G By Google

Overview   Privacy practices   Reviews   Related

User Reviews   Write a review   English   Helpful

Alpine Observer   Modified Aug 6, 2017   ★★★★★

After several days of using this extension I then recently noticed that Chrome was not connecting to the internet at all, no sites at all. Other browsers were working OK. I spent over an hour troubleshooting, but no joy.

Then, I disabled all extensions, and Chrome starting working again. So I re-enabled all other extensions and Chrome kept on working....until I re-enabled this extension, then it stopped connecting to the internet entirely again!

So now this extension is disabled, and meanwhile Google keep on sucking up all my browsing information and invading my privacy.

I concluded that Google perhaps have ZERO interest in making this an effective extension because it reduces how much of your information and privacy they can steal?

Was this review helpful? ○ Yes   ○ No   Reply | Mark as spam or abuse

Hexane Smith   Feb 2, 2022

Google knows me better than anyone else, better than even I do.
Look on the bright side - after we die, we can live again once they figure out how to sort all of this information into a coherent being. Which can be advertised to for all eternity!
(Seriously, I hope whatever AI takes over they make sure that no semi-eternal synthetic lifeforms are capable of semi-eternal suffering. At least with us meatbags it's limited to 110 years max).

Was this review helpful? ○ Yes   ○ No | Mark as spam or abuse

Abinash Senapati   Sep 14, 2017

Do you have a dynamic ip or just a static one. For static just add filter in google analytics itself and for the dynamic if this extension not working as you have already said then just add a custom filter in google analytics as "user defined-cookie_filter" :)

Was this review helpful? ○ Yes   ○ No | Mark as spam or abuse

Paulie Webster   Modified Oct 7, 2016   ★★★★★

Works perfectly. Lots of bad reviews saying it doesn't work. Not sure why, maybe people think it removes the code from your webpage? That's not how the internet works? This extension tells the analytics code not to fire. I just tested it on my site, and with the extension enabled, Google Analytics Real-Time didn't see my site views or my contact form goal conversions. But when I disabled the extension, Analytics could see me again. As far as I can tell this works perfectly. Thanks!

Was this review helpful? ○ Yes   ○ No   Reply | Mark as spam or abuse

chrome web store   ⚙ Sign in

Home > Extensions > Google Analytics Opt-out Add-on (by Google)

Google Analytics Opt-out Add-on (by Google)   Available on Chrome

◎ Featured

★★★★☆ 1,730 | Search Tools | 1,000,000+ users

G By Google

Overview   Privacy practices   Reviews   Related

User Reviews   Write a review   English   Helpful

Alpine Observer Modified Aug 6, 2017 ★★★★★

After several days of using this extension I then recently noticed that Chrome was not connecting to the internet at all, no sites at all. Other browsers were working OK. I spent over an hour troubleshooting, but no joy.

Then, I disabled all extensions, and Chrome starting working again. So I re-enabled all other extensions and Chrome kept on working....until I re-enabled this extension, then it stopped connecting to the internet entirely again!

So now this extension is disabled, and meanwhile Google keep on sucking up all my browsing information and invading my privacy.

I concluded that Google perhaps have ZERO interest in making this an effective extension because it reduces how much of your information and privacy they can steal?

Was this review helpful? ○ Yes   ○ No   Reply | Mark as spam or abuse

Hexane Smith Feb 2, 2022

Google knows me better than anyone else, better than even I do.
Look on the bright side - after we die, we can live again once they figure out how to sort all of this information into a coherent being. Which can be advertised to for all eternity!
(Seriously, I hope whatever AI takes over they make sure that no semi-eternal synthetic lifeforms are capable of semi-eternal suffering. At least with us meatbags it's limited to 110 years max).

Was this review helpful? ○ Yes   ○ No | Mark as spam or abuse

Abinash Senapati Sep 14, 2017

Do you have a dynamic ip or just a static one. For static just add filter in google analytics itself and for the dynamic if this extension not working as you have already said then just add a custom filter in google analytics as "user defined-cookie_filter" :)

Was this review helpful? ○ Yes   ○ No | Mark as spam or abuse

Paulie Webster Modified Oct 7, 2016 ★★★★★

Works perfectly. Lots of bad reviews saying it doesn't work. Not sure why, maybe people think it removes the code from your webpage? That's not how the internet works? This extension tells the analytics code not to fire. I just tested it on my site, and with the extension enabled, Google Analytics Real-Time didn't see my site views or my contact form goal conversions. But when I disabled the extension, Analytics could see me again. As far as I can tell this works perfectly. Thanks!

Was this review helpful? ○ Yes   ○ No   Reply | Mark as spam or abuse

 chrome web store   ⚙ Sign in

Home > Extensions > Google Analytics Opt-out Add-on (by Google)

Google Analytics Opt-out Add-on (by Google)

Available on Chrome

📍 Featured

★★★★☆ 1,730 | Search Tools | 1,000,000+ users

G By Google

Overview   Privacy practices   Reviews   Related

User Reviews   Write a review

English   Helpful

Alpine Observer   Modified Aug 6, 2017   ★★★★★

After several days of using this extension I then recently noticed that Chrome was not connecting to the internet at all, no sites at all. Other browsers were working OK. I spent over an hour troubleshooting, but no joy.

Then, I disabled all extensions, and Chrome starting working again. So I re-enabled all other extensions and Chrome kept on working....until I re-enabled this extension, then it stopped connecting to the internet entirely again!

So now this extension is disabled, and meanwhile Google keep on sucking up all my browsing information and invading my privacy.

I concluded that Google perhaps have ZERO interest in making this an effective extension because it reduces how much of your information and privacy they can steal?

Was this review helpful? ○ Yes   ○ No   Reply | Mark as spam or abuse

Hexane Smith   Feb 2, 2022

Google knows me better than anyone else, better than even I do.
Look on the bright side - after we die, we can live again once they figure out how to sort all of this information into a coherent being. Which can be advertised to for all eternity!
(Seriously, I hope whatever AI takes over they make sure that no semi-eternal synthetic lifeforms are capable of semi-eternal suffering. At least with us meatbags it's limited to 110 years max).

Was this review helpful? ○ Yes   ○ No | Mark as spam or abuse

Abinash Senapati   Sep 14, 2017

Do you have a dynamic ip or just a static one. For static just add filter in google analytics itself and for the dynamic if this extension not working as you have already said then just add a custom filter in google analytics as "user defined-cookie_filter" :)

Was this review helpful? ○ Yes   ○ No | Mark as spam or abuse

Paulie Webster   Modified Oct 7, 2016   ★★★★★

Works perfectly. Lots of bad reviews saying it doesn't work. Not sure why, maybe people think it removes the code from your webpage? That's not how the internet works? This extension tells the analytics code not to fire. I just tested it on my site, and with the extension enabled, Google Analytics Real-Time didn't see my site views or my contact form goal conversions. But when I disabled the extension, Analytics could see me again. As far as I can tell this works perfectly. Thanks!

Was this review helpful? ○ Yes   ○ No   Reply | Mark as spam or abuse

chrome web store   ⚙ Sign in

Home > Extensions > Google Analytics Opt-out Add-on (by Google)

Google Analytics Opt-out Add-on (by Google)   Available on Chrome

📍 Featured

★★★★☆ 1,730 | Search Tools | 1,000,000+ users

G By Google

Overview   Privacy practices   Reviews   Related

User Reviews   Write a review   English   Helpful

Alpine Observer   Modified Aug 6, 2017   ★★★★★

After several days of using this extension I then recently noticed that Chrome was not connecting to the internet at all, no sites at all. Other browsers were working OK. I spent over an hour troubleshooting, but no joy.

Then, I disabled all extensions, and Chrome starting working again. So I re-enabled all other extensions and Chrome kept on working....until I re-enabled this extension, then it stopped connecting to the internet entirely again!

So now this extension is disabled, and meanwhile Google keep on sucking up all my browsing information and invading my privacy.

I concluded that Google perhaps have ZERO interest in making this an effective extension because it reduces how much of your information and privacy they can steal?

Was this review helpful? ○ Yes   ○ No   Reply | Mark as spam or abuse

> **Hexane Smith**   Feb 2, 2022
>
> Google knows me better than anyone else, better than even I do.
> Look on the bright side - after we die, we can live again once they figure out how to sort all of this information into a coherent being. Which can be advertised to for all eternity!
> (Seriously, I hope whatever AI takes over they make sure that no semi-eternal synthetic lifeforms are capable of semi-eternal suffering. At least with us meatbags it's limited to 110 years max).
>
> Was this review helpful? ○ Yes   ○ No | Mark as spam or abuse
>
> **Abinash Senapati**   Sep 14, 2017
>
> Do you have a dynamic ip or just a static one. For static just add filter in google analytics itself and for the dynamic if this extension not working as you have already said then just add a custom filter in google analytics as "user defined-cookie_filter" :)
>
> Was this review helpful? ○ Yes   ○ No | Mark as spam or abuse

Paulie Webster   Modified Oct 7, 2016   ★★★★★

Works perfectly. Lots of bad reviews saying it doesn't work. Not sure why, maybe people think it removes the code from your webpage? That's not how the internet works? This extension tells the analytics code not to fire. I just tested it on my site, and with the extension enabled, Google Analytics Real-Time didn't see my site views or my contact form goal conversions. But when I disabled the extension, Analytics could see me again. As far as I can tell this works perfectly. Thanks!

Was this review helpful? ○ Yes   ○ No   Reply | Mark as spam or abuse

The **Record.**
BY RECORDED FUTURE

Catalin Cimpanu | October 23, 2021

Malware found in npm package with millions of weekly downloads

Malware   News   Technology

A massively popular JavaScript library (npm package) was hacked today and modified with malicious code that downloaded and installed a password stealer and cryptocurrency miner on systems where the compromised versions were used.

- The incident was detected on Friday, October 22.
- It impacted UAParser.js, a JavaScript library for reading information stored inside user-agent strings.
- According to its official site, the library is used by companies such as Facebook, Apple, Amazon, Microsoft, Slack, IBM, HPE, Dell, Oracle, Mozilla, Shopify, Reddit, and many of Silicon Valley's elites.
- The library also regularly sees between 6 million and 7 million weekly downloads, according to its npm page.
- **Compromised versions:** 0.7.29, 0.8.0, 1.0.0
- **Patched versions:** 0.7.30, 0.8.1, 1.0.1

"I believe someone was hijacking my npm account and published some compromised packages (0.7.29, 0.8.0, 1.0.0) which will probably install malware," said Faisal Salman, author of the UAParser.js library.

Hours after discovering the hack, Salman pulled the compromised library versions—to prevent users from accidentally infecting themselves—and released clean ones.

Analysis of the malicious code revealed extra scripts that would download and execute binaries from a remote server. Binaries were provided for both Linux and Windows platforms.

"From the command-line arguments, one of them looks like a cryptominer, but that might be just for camouflage," a GitHub user said on Friday.

But on Windows systems, the scripts would also download and execute an infostealer trojan (possibly a version of the Danabot malware) that contained functionality to export browser cookies, browser passwords, and OS credentials, according to another GitHub user's findings.

Because of the large number of downloads and the big-name corporations that relied on the library, the US Cybersecurity and Infrastructure Security Agency (CISA) published a security alert late Friday night about the incident, urging developers to update to the safe versions.

GitHub's security team also took note of the incident and issued its own adviory, urging immediate password resets and token rotations from systems where the library was used part of development processes.

Any computer that has this package installed or running should be considered fully compromised. All secrets and keys stored on that computer should be rotated immediately from a different computer. The package should be removed, but as full control of the computer may have been given to an outside entity, there is no guarantee that removing the package will remove all malicious software resulting from installing it.

This marks the fourth malicious npm package found this week. On Wednesday, Sonatype also found three newly-released npm libraries that contained similar malicious code, intended to download and install a cryptocurrency miner, targeting Linux and Windows systems alike.

Article updated at 13:30pm, October 23, to add that a password-stealing trojan was also discovered inside the compromised library.

Tags

crypto-miner   GitHub   JavaScript   malware   npm   programming   webdev

Catalin Cimpanu is a cybersecurity reporter for The Record. He previously worked at ZDNet and Bleeping Computer, where he became a well-known name in the industry for his constant scoops on new vulnerabilities, cyberattacks, and law enforcement actions against hackers.

‹ Previous article   Next article ›

BRIEFS

Agricultural equipment maker AGCO reports ransomware attack | May 6, 2022

Avast, AVG release security updates for decade-old vulnerability | May 6, 2022

Cyberattack takes down network of State Bar of Georgia | May 5, 2022

CISA urges F5 users to address 'critical' vulnerability in BIG-IP software | May 5, 2022

FBI: Business Email Compromise attacks led to more than $43 billion in losses since 2016 | May 4, 2022

By end of 2023, GitHub to force code contributors to use two-factor authentication | May 4, 2022

White House wants nation to prepare for cryptography-breaking quantum computers | May 4, 2022

Classes resume at Michigan community college after ransomware attack | May 4, 2022

RANSOMWARE TRACKER: THE LATEST FIGURES [APRIL 2022]

Victim Data Released on Ransomware Extortion Sites
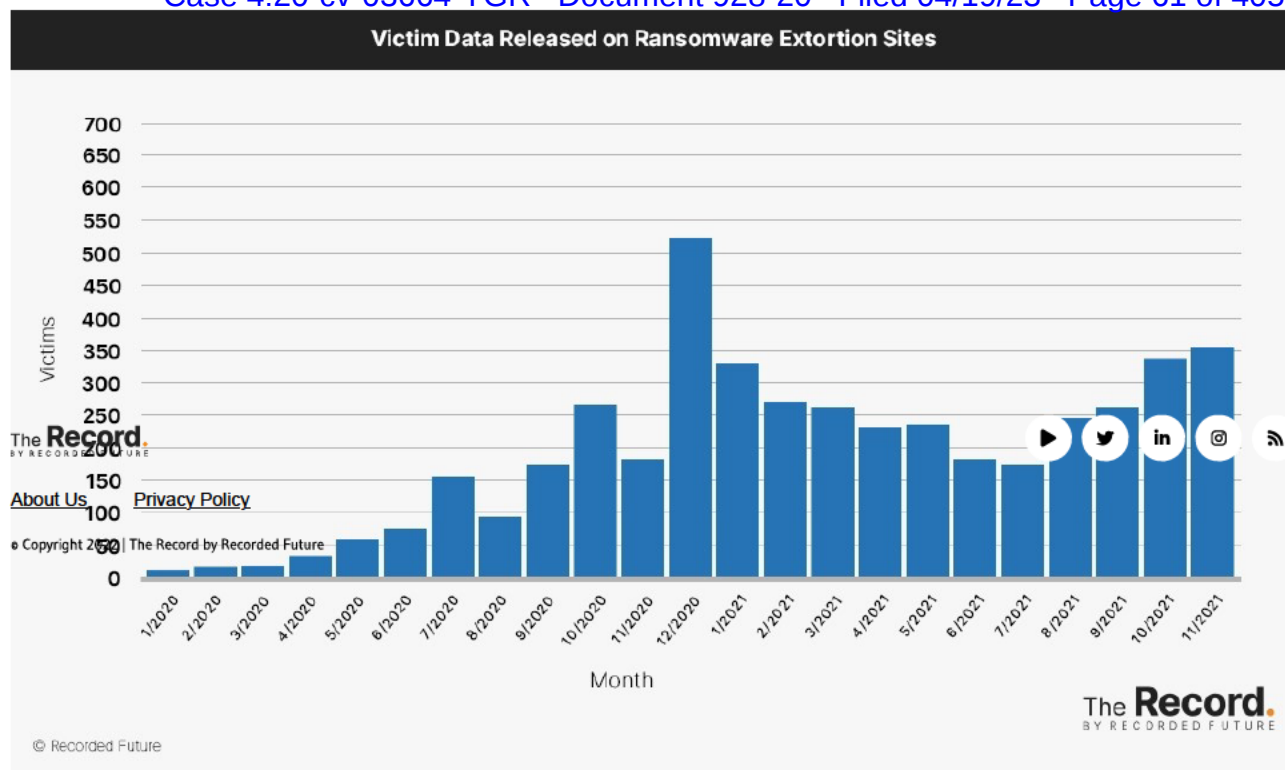
RANSOMWARE TRACKER: THE LATEST FIGURES [APRIL 2022]

Google Analytics stops logging IP addresses: here's why it's a big deal for marketers

By Kendra Clark - March 16, 2022

By announcing the elimination of IP address logging on Google Analytics, the tech titan is doubling down on its focus on consumer data privacy. While some applaud the move, other see it as a headache for advertisers and another nail in the coffin of digital marketing as we know it.

Google is axing Internet Protocol (IP) address logging on its analytics platform. The decision could hamper marketing effectiveness by cutting off advertisers' ability to access user location data, but experts say it's a sensical move in the broader context of maturing privacy standards.

An IP address is a unique identifier that allows Google, and others, to locate an individual user's device on the internet or a local network. Advertisers rely on this information for targeting – but its days on Google's analytics platform are numbered.

The move is part of a larger decision announced today, which will see Google Analytics 4 (GA4) take the place of Universal Analytics (UA) and Universal Analytics 360 for all Google customers beginning next year. In a statement shared with The Drum, the company said the decision was made in response to "a monumental shift in the way people behave on the internet and ... how we measure that behavior." In essence, Google sees the UA platform as increasingly outdated due to its reliance on third-party cookies – which are disappearing as fast as the long winter days. Instead of cookies, GA4 will employ an event-based framework, which aggregates data from specific instances of user interaction to generate modeled data that's easy to query. The shift aims to enable seamless operations across platforms. GA4 also offers a range of new, valuable integrations across Search, Google Cloud, YouTube, Google Display & Video 360 and more.

But the company noted that the decision to shift to GA4 also has to do with "the constantly evolving privacy landscape." As part of Google's efforts to address the changing privacy space, the new iteration of its analytics platform will no longer store user IP addresses. The move represents a major shift away from long-standing tracking-based models of data collection, advertising and campaign measurement, and reinforces Google's increasingly stringent privacy stance.

Some marketers are already worrying that the decision to eliminate IP address logging in GA4 will hamper ad targeting and measurement. They've already seen this occur as a result of Apple's privacy-centric iOS changes – such as [its AppTrackingTransparency policy](#), which gives users more say over the apps and websites with which they share their personal information.

Russell Ketchum, director of product at Google Analytics, says that tracking IP addresses is simply no longer necessary, since GA4 is equipped with other tools to help marketers optimize performance. "We're not logging or storing IP addresses because we no longer need to," he tells The Drum. "When we introduced Google Analytics 4 [in October of 2020], we made it clear that there was a core focus on end-user privacy. IP addresses have been anonymized in Google Analytics 4 since it launched and, with this new announcement, we're going even further and removing IP addresses altogether. This change won't impact the quality of customers' reports."

And for many, the change comes as no surprise. "Google has been developing this new analytics

platform for more than three years now, so … [the news] isn't completely unexpected," says Charles Farina, head of innovation at Adswerve, a firm specializing in Google marketing and analytics. "The company has made the decision to sunset Universal Analytics for Google Analytics 4 in direct response to consumer data privacy preferences and evolving marketing strategies that do not lean on third-party cookies. This is a shift from a session-oriented model to an event-based model that better aligns with how companies are looking to measure user engagement with their digital marketing content in the future."

Beyond Google's ongoing efforts to improve consumer data privacy standards by phasing out the third-party cookie come 2023 and abandoning last-click attribution for a machine-learning-based model as the standard yardstick for marketers, the broader cultural shift toward more stringent privacy norms is well under way. Following the implementation of the EU's General Data Protection Regulation (GDPR) in 2018, the international community has seen a proliferation of similar national and state-level laws both proposed and passed that have introduced new protections and controls for consumers but have limited business' ability to collect, store, sell and use consumers' personal information. For advertisers in particular, the stakes have grown exponentially higher with new user privacy policies implemented by tech players such as Google and Apple.

Although it's been a leader in determining the future of consumer data standards and norms, Google itself has come under fire a few times over the last couple of years for failing to adhere to privacy standards – including as recently as December.

Google Analytics in particular has been the subject of some controversy amid Schrems II, the EU's landmark data protection verdict issued in July of 2020, which, for surveillance reasons, prohibits Europeans' data from being shared with US servers. The new GA4, however, will offer country-level controls that allow its use to be customized according to local and state-level regulations. This change could help the platform gain adoption in Europe; previously, many EU policymakers have forbidden its use due to the classification of IP addresses as protected personal data under Schrems II.

Plus, earlier this year, both the Austrian Data Protection Authority and France's Commission nationale de l'informatique et des libertés have cracked down on privacy in two cases involving Google Analytics.

The decision to ban IP address logging on Google Analytics 4, then, is seen by some as a strategic move by Google made in response to backlash faced in Europe. "In light of the recent Google Analytics decisions in Europe, and in particular, the Austrian Data Protection Authority's emphasis on the failure of the website operator to properly implement IP 'anonymization,' the IP address change is likely a timely effort to mitigate such risk while awaiting resolution on the broader issue of EU-US transfers," says Arielle Garcia, chief privacy officer at UM Worldwide. "The GA4 privacy controls, and their country-level settings, will be useful for brands as they consider refining their privacy approach – for example, ahead of the new state laws that will be operable in 2023."

Others argue that marketers who are already on the ball won't see much of a practical difference in the platform's new privacy changes. "The privacy features being added to GA4, such as IP address redaction, have little or no penalty," Doug Hall, senior director of analytics EMEA at Media.Monks, says. "The industry has known for the best part of a decade what data with purpose looks like, and the loss of IP address resolution is inconsequential for analysts and marketers, with only upside for the users."

At this point in the game, most savvy marketers have moved beyond reliance on the location and ISP information gained from tracking user IP addresses, according to Hall. Plus, he says, the industry's growing attention to consumer data privacy will naturally fuel innovation.

GA4 will only equip marketers to better prepare for the cookieless future, says Hall. "GA4 has more integrations and more features for first-class first-party data gathering – there's every reason to believe that in 12 months, we'll look back at the session-based, page view-oriented, artificial constructs that the old data model imposed and we'll be thankful for change. The trajectory is clear, if not immediately welcomed by all."

Universal Analytics will be officially phased out on July 1 2023 and Universal Analytics 360 will follow on October 1 2023. Google declined a request for comment.

For more, sign up for The Drum's daily US newsletter here.

+ ENGLISH

MOTHERBOARD
TECH BY VICE

Data Broker Is Selling Location Data of People Who Visit Abortion Clinics

It costs just over $160 to get a week's worth of data on where people who visited Planned Parenthood came from, and where they went afterwards.

By Joseph Cox

May 3, 2022, 12:46pm   [f]   [twitter]   [snapchat]

+ ENGLISH

IMAGE: THE WASHINGTON POST/CONTRIBUTOR

A location data firm is selling information related to visits to clinics that provide abortions including Planned Parenthood facilities, showing where groups of people visiting the locations came from, how long they stayed there, and where they then went afterwards, according to sets of the data purchased by Motherboard.

The data sale is obviously more important in the context of a leaked Supreme Court draft opinion in which Justice Alito indicated that the court is ready to repeal the decision in *Roe v. Wade*, the decades-old precedent that has provided federal protections to those seeking an abortion. If that draft does become a formal decision, it would immediately fully or partly ban abortion rights in at least 13 states.

Hacking. Disinformation. Surveillance. CYBER is Motherboard's podcast and reporting on the dark underbelly of the internet.

SEE MORE →

How data collecting intersects with abortion rights, or the lack thereof, is likely to gather more attention in the wake of the draft. The country may also see an

+ ENGLISH

as well. Anti-abortion groups are already fairly adept at using novel technology for their goals. In 2016, an advertising CEO who worked with anti-abortion and Christian groups sent targeted advertisements to women sitting in Planned Parenthood clinics in an attempt to change their decision around getting an abortion. The sale of the location data raises questions around why companies are selling data based on abortion clinics specifically, and whether they should introduce more safeguards around the purchase of that information, if be selling it at all.

"It's bonkers dangerous to have abortion clinics and then let someone buy the census tracks where people are coming from to visit that abortion clinic," Zach Edwards, a cybersecurity researcher who closely tracks the data selling marketplace, told Motherboard in an online chat after reviewing the data. "This is how you dox someone traveling across state lines for abortions—how you dox clinics providing this service."

> *Do you work in the location data industry or how know else the data is being used? We'd love to hear from you. Using a non-work phone or computer, you can contact Joseph Cox securely on Signal on +44 20 8133 5190, Wickr on josephcox, OTR chat on jfcox@jabber.ccc.de, or email joseph.cox@vice.com.*

In the wake of a near-total abortion ban in Texas, for example, people in Texas seeking abortions have increasingly had to travel to other states where abortion access is easier to get the care they need. With *Roe* set to fall, people seeking abortions who live in conservative states and can afford to are likely to start traveling to get an abortion. Location data could play into whether and how that travel is identified, making it even more urgent for regulators and lawmakers to consider how location data is collected, used, and sold.

+ ENGLISH

install code, called software development kits (SDKs), into their apps that sends users' location data to companies in exchange for the developer receiving payment. Sometimes app users don't know that their phone—be that via a prayer app, or a weather app—is collecting and sending location data to third parties, let alone some of the more dangerous use cases that Motherboard has reported on, including transferring data to U.S. military contractors. Planned Parenthood is not the organization performing the data collection nor benefiting from it financially.

SafeGraph then repackages that location data and other data into various products. On Tuesday Motherboard reported that the CDC bought $420,000 worth of SafeGraph data for a laundry list of COVID-19 and non-COVID-19 use cases. Google banned SafeGraph from the Google Play Store in June.

SafeGraph classifies "Planned Parenthood" as a "brand" that can be tracked, and the data Motherboard purchased includes more than 600 Planned Parenthood locations in the United States. The data included a week's worth of location data for those locations in mid-April. SafeGraph calls the location data product "Patterns." In total, the data cost just over $160. Not all Planned Parenthood locations offer abortion services. But Motherboard verified that some facilities included in the purchased dataset do.

Motherboard also searched the SafeGraph website for "Family Planning," which returned a relevant result of "Family Planning Centers" that people could then buy data related to.

SafeGraph's Patterns data aims to answer questions like "how often people visit, how long they stay, where they

Tech

CDC Tracked Millions of Phones to See If Americans Followed COVID Lockdown Orders

+ ENGLISH

SafeGraph does this by analyzing where a phone is commonly located overnight, the company's documentation suggests.

SafeGraph's data is aggregated, meaning it isn't explicitly specifying where a certain device moved to. Instead, it focuses on the movements of groups of devices. But researchers have repeatedly warned about the possibilities of unmasking individuals contained in allegedly anonymized datasets.

Sections of the SafeGraph dataset Motherboard purchased handle a very small number of devices per record, theoretically making deanonymization of those people easier. Some had just four or five devices visiting that location, with SafeGraph filtering the data by whether the person used an Android or an iOS device as well.

On the data showing where people traveled to a certain clinic based on their census block, potentially across state borders, Edwards said "SafeGraph is going to be the weapon of choice for anti-choice radicals attempting to target 'out of state clinics' providing medical care." Missouri is considering a law to make it illegal to "aid or abet" abortions in other states.

Tech

Google Bans Location Data Firm Funded by Former Saudi Intelligence Head

JOSEPH COX

08.12.21

Tracking visitors to abortion clinics has long been a staple in showing the threat posed by location data. In a 2018 investigation, *The New York Times* took location data and followed multiple people inside it, and unmasked some of those. One of the people followed visited a Planned Parenthood facility, according to the report.

Recently, a Christian-focused outlet The Pillar published a piece that used

+ ENGLISH

Planned Parenthood did not respond to a request for comment. SafeGraph did not respond to a request for comment either, which included the specific question of whether the company would continue to sell location data related to abortion clinics.

Subscribe to our cybersecurity podcast, CYBER. Subscribe to our new Twitch channel.

TAGGED: SURVEILLANCE, PRIVACY, PLANNED PARENTHOOD, CYBER, ROE V. WADE, ABORTION RIGHTS, LOCATION DATA, CELLPHONE LOCATION DATA

ORIGINAL REPORTING ON EVERYTHING THAT MATTERS IN YOUR INBOX.

> Your email address

By signing up, you agree to the Terms of Use and Privacy Policy & to receive electronic communications from Vice Media Group, which may include marketing promotions, advertisements and sponsored content.

MORE FROM VICE

+ ENGLISH

JOSEPH COX

05.04.22

Tech

Location Data Firm Provides Heat Maps of Where Abortion Clinic Visitors Live

JOSEPH COX

05.05.22

Tech

16 Senators Push FTC: What Are You Doing to Protect Location Data of Women Seeking Abortions?

JOSEPH COX

05.23.22

Tech

SafeGraph Investor Selling His Stake, Donating the Money to Planned Parenthood

JOSEPH COX

05.05.22

Tech

Over 40 Members of Congress Urge Google to Limit Location Data Collection for a Post-Roe America

JOSEPH COX

05.24.22

Tech

Data Marketplace Selling Info About Who Uses Period Tracking Apps

JOSEPH COX

05.17.22

+ ENGLISH

+ ENGLISH

+ ENGLISH

+ ENGLISH

PARTNER

VICE VOICES

CONTENT FUNDING ON VICE

SECURITY POLICY

PRIVACY & TERMS

ACCESSIBILITY STATEMENT

© 2022 VICE MEDIA GROUP

INDEPENDENT

Contribute   Subscribe   LOGIN

Tech

Google Chrome's private incognito mode leaks way more personal data than you might think

The privacy feature in the Chrome web browser claims to let people 'browse privately'

Anthony Cuthbertson   •   Wednesday 22 August 2018 12:13   •   ••• Comments
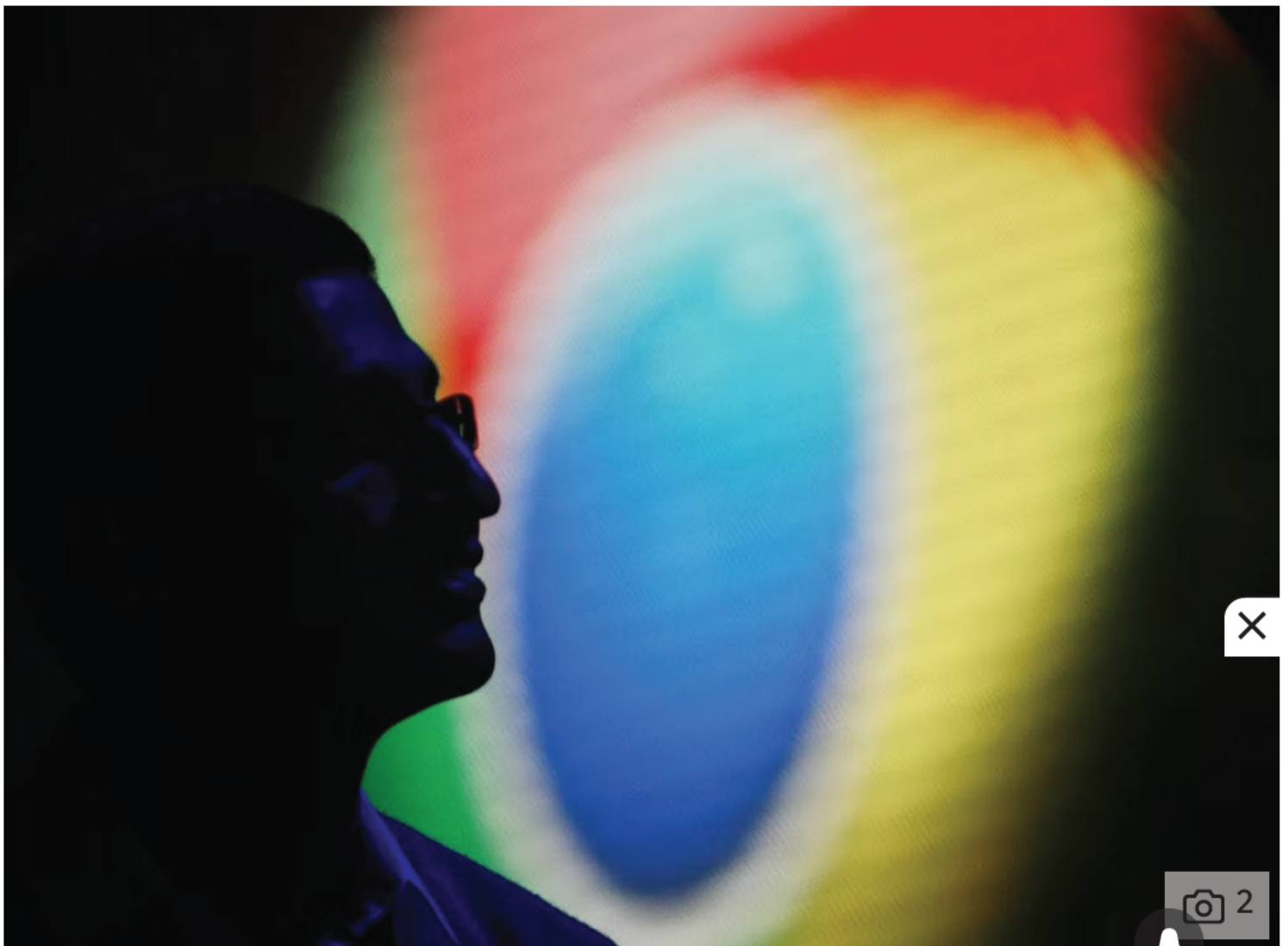
Incognito mode in Chrome claims to let users browse the web privately without Google collecting their information

INDEPENDENT

Contribute   Subscribe   LOGIN

BREAKING NEWS

Please enter your email here   SIGN UP

I would like to be emailed about offers, events and updates from
The Independent. Read our privacy notice

Google could continue to collect personal data from users, even if they use the incognito mode in the Chrome web browser, a study has found.

A researcher from Vanderbilt University in Nashville, Tennessee, discovered that Google could retroactively link a person's private browsing to the usernames and account information they use online.

Register for free to continue reading

Registration is a free and easy way to support our truly independent journalism

By registering, you will also enjoy limited access to Premium articles, exclusive newsletters, commenting, and virtual events with our leading journalists

Email

Enter your email

Password

Enter your password

Must be at least 6 characters, include an upper and lower case character and a number

First name

Enter your first name

Last name

Enter your last name

Year of birth

Select your year of birth

INDEPENDENT   ☰

Contribute   Subscribe   **LOGIN**

Opt-out-policy   ⌄

REGISTER   I'LL TRY LATER

Already have an account? sign in

By clicking Regi ter you confirm that your data ha been entered correctly and you have read and agree to our **Terms of use, Cookie policy** and **Privacy notice**

Thi   ite i protected by reCAPTCHA and the Google **Privacy policy** and **Terms of service** apply

More about: Google

Join our new commenting forum
Join thought-provoking conversations, follow other Independent readers and see their replies

💬 **Comments** ↓

Contribute   Subscribe

LOGIN

✕

INDEPENDENT

INDEPENDENT

Contribute   Subscribe

LOGIN

GET IN TOUCH

Contact us

Jobs

OUR PRODUCTS

Subscribe

Register

Newsletters

Donate

Install our app

Archive

OTHER PUBLICATIONS

International editions

Independent en Español

Independent Arabia

INDEGENDENT

Contribute   Subscribe   LOGIN

Novaya Gazeta

LEGAL   **EXTRAS**

Code of conduct and complaints   All topics

Contributors   Voucher codes

Cookie policy   Compare

Donations Terms & Conditions   Independent Advertising

Privacy notice   Syndication

Privacy settings   Working at The Independent

User policies

Modern Slavery Act

ELECTRONIC FRONTIER FOUNDATION

How Unique Is Your Web Browser?

Peter Eckersley[*]

Electronic Frontier Foundation,
pde@eff.org

Abstract. We investigate the degree to which modern web browsers are subject to "device fingerprinting" via the version and configuration information that they will transmit to websites upon request. We implemented one possible fingerprinting algorithm, and collected these fingerprints from a large sample of browsers that visited our test side, `panopticlick.eff.org`. We observe that the distribution of our fingerprint contains at least 18.1 bits of entropy, meaning that if we pick a browser at random, at best we expect that only one in 286,777 other browsers will share its fingerprint. Among browsers that support Flash or Java, the situation is worse, with the average browser carrying at least 18.8 bits of identifying information. 94.2% of browsers with Flash or Java were unique in our sample.

By observing returning visitors, we estimate how rapidly browser fingerprints might change over time. In our sample, fingerprints changed quite rapidly, but even a simple heuristic was usually able to guess when a fingerprint was an "upgraded" version of a previously observed browser's fingerprint, with 99.1% of guesses correct and a false positive rate of only 0.86%.

We discuss what privacy threat browser fingerprinting poses in practice, and what countermeasures may be appropriate to prevent it. There is a tradeoff between protection against fingerprintability and certain kinds of debuggability, which in current browsers is weighted heavily against privacy. Paradoxically, anti-fingerprinting privacy technologies can be self-defeating if they are not used by a sufficient number of people; we show that some privacy measures currently fall victim to this paradox, but others do not.

1 Introduction

It has long been known that many kinds of technological devices possess subtle but measurable variations which allow them to be "fingerprinted". Cameras [1,2], typewriters [3], and quartz crystal clocks [4,5] are among the devices that can be

---

2

entirely or substantially identified by a remote attacker possessing only outputs or communications from the device.

There are several companies that sell products which purport to fingerprint web browsers in some manner [6,7], and there are anecdotal reports that these prints are being used both for analytics and second-layer authentication purposes. But, aside from limited results from one recent experiment [8], there is to our knowledge no information in the public domain to quantify how much of a privacy problem fingerprinting may pose.

In this paper we investigate the real-world effectiveness of browser fingerprinting algorithms. We defined one candidate fingerprinting algorithm, and collected these fingerprints from a sample of 470,161 browsers operated by informed participants who visited the website https://panopticlick.eff.org. The details of the algorithm, and our collection methodology, are discussed in Section 3. While our sample of browsers is quite biased, it is likely to be representative of the population of Internet users who pay enough attention to privacy to be aware of the minimal steps, such as limiting cookies or perhaps using proxy servers for sensitive browsing, that are generally agreed to be necessary to avoid having most of one's browsing activities tracked and collated by various parties.

In this sample of privacy-conscious users, 83.6% of the browsers seen had an instantaneously unique fingerprint, and a further 5.3% had an anonymity set of size 2. Among visiting browsers that had either Adobe Flash or a Java Virtual Machine enabled, 94.2% exhibited instantaneously unique fingerprints and a further 4.8% had fingerprints that were seen exactly twice. Only 1.0% of browsers with Flash or Java had anonymity sets larger than two. Overall, we were able to place a lower bound on the fingerprint distribution entropy of 18.1 bits, meaning that if we pick a browser at random, at best only one in 286,777 other browsers will share its fingerprint. Our results are presented in further detail in Section 4.

In our data, fingerprints changed quite rapidly. Among the subset of 8,833 users who accepted cookies and visited panopticlick.eff.org several times over a period of more than 24 hours, 37.4% exhibited at least one fingerprint change. This large percentage may in part be attributable to the interactive nature of the site, which immediately reported the uniqueness or otherwise of fingerprints and thereby encouraged users to find ways to alter them, particularly to try to make them less unique. Even if 37.4% is an overestimate, this level of fingerprint instability was at least momentary grounds for privacy optimism.

Unfortunately, we found that a simple algorithm was able to guess and follow many of these fingerprint changes. If asked about all newly appearing fingerprints in the dataset, the algorithm was able to correctly pick a "progenitor" fingerprint in 99.1% of cases, with a false positive rate of only 0.87%. The analysis of changing fingerprints is presented in Section 5.

Online Tracking:
A 1-million-site Measurement and Analysis

Steven Englehardt
Princeton University
ste@cs.princeton.edu

Arvind Narayanan
Princeton University
arvindn@cs.princeton.edu

ABSTRACT

We present the largest and most detailed measurement of online tracking conducted to date, based on a crawl of the top 1 million websites. We make 15 types of measurements on each site, including stateful (cookie-based) and stateless (fingerprinting-based) tracking, the effect of browser privacy tools, and the exchange of tracking data between different sites ("cookie syncing"). Our findings include multiple sophisticated fingerprinting techniques never before measured in the wild.

This measurement is made possible by our open-source web privacy measurement tool, OpenWPM[1], which uses an automated version of a full-fledged consumer browser. It supports parallelism for speed and scale, automatic recovery from failures of the underlying browser, and comprehensive browser instrumentation. We demonstrate our platform's strength in enabling researchers to rapidly detect, quantify, and characterize emerging online tracking behaviors.

1. INTRODUCTION

Web privacy measurement — observing websites and services to detect, characterize and quantify privacy-impacting behaviors — has repeatedly forced companies to improve their privacy practices due to public pressure, press coverage, and regulatory action [5, 13]. On the other hand, web privacy measurement presents formidable engineering and methodological challenges. In the absence of a generic tool, it has been largely confined to a niche community of researchers.

We seek to transform web privacy measurement into a widespread practice by creating a tool that is useful not just to our colleagues but also to regulators, self-regulators, the press, activists, and website operators, who are often in the dark about third-party tracking on their own domains. We also seek to lessen the burden of *continual* oversight of web tracking and privacy, by developing a robust and modular platform for repeated studies.

[1]https://github.com/citp/OpenWPM

OpenWPM (Section 3) solves three key systems challenges faced by the web privacy measurement community. It does so by building on the strengths of past work, while avoiding the pitfalls made apparent in previous engineering efforts. (1) We achieve scale through parallelism and robustness by utilizing isolated measurement processes similar to FPDetective's platform [2], while still supporting stateful measurements. We're able to scale to 1 million sites, without having to resort to a stripped-down browser [22] (a limitation we explore in detail in Section 3.3). (2) We provide comprehensive instrumentation by expanding on the rich browser extension instrumentation of FourthParty [23], without requiring the researcher to write their own automation code. (3) We reduce duplication of work by providing a modular architecture to enable code re-use between studies.

Solving these problems is hard because the web is not designed for automation or instrumentation. Selenium,[2] the main tool for automated browsing through a full-fledged browser, is intended for developers to test their *own* websites. As a result it performs poorly on websites not controlled by the user and breaks frequently if used for large-scale measurements. Browsers themselves tend to suffer memory leaks over long sessions. In addition, *instrumenting* the browser to collect a variety of data for later analysis presents formidable challenges. For full coverage, we've found it necessary to have three separate measurement points: a network proxy, a browser extension, and a disk state monitor. Further, we must link data collected from these disparate points into a uniform schema, duplicating much of the browser's own internal logic in parsing traffic.

A large-scale view of web tracking and privacy.

In this paper we report results from a January 2016 measurement of the top 1 million sites (Section 4). Our scale enables a variety of new insights. We observe for the first time that online tracking has a "long tail", but we find a surprisingly quick drop-off in the scale of individual trackers: trackers in the tail are found on very few sites (Section 5.1). Using a new metric for quantifying tracking (Section 5.2), we find that the tracking-protection tool Ghostery (https://www.ghostery.com/) is effective, with some caveats (Section 5.5). We quantify the impact of trackers and third parties on HTTPS deployment (Section 5.3) and show that cookie syncing is pervasive (Section 5.6).

Turning to browser fingerprinting, we revisit an influential 2014 study on canvas fingerprinting [1] with updated and improved methodology (Section 6.1). Next, we report on several types of fingerprinting never before measured at scale:

[2]http://www.seleniumhq.org/

font fingerprinting using canvas (which is distinct from canvas fingerprinting; Section 6.2), and fingerprinting by abusing the WebRTC API (Section 6.3), the Audio API (Section 6.4), and the Battery Status API (6.5). Finally, we show that in contrast to our results in Section 5.5, existing privacy tools are *not* effective at detecting these newer and more obscure fingerprinting techniques.

Overall, our results show cause for concern, but also encouraging signs. In particular, several of our results suggest that while online tracking presents few barriers to entry, trackers in the tail of the distribution are found on very few sites and are far less likely to be encountered by the average user. Those at the head of the distribution, on the other hand, are owned by relatively few companies and are responsive to the scrutiny resulting from privacy studies.

We envision a future where measurement provides a key layer of oversight of online privacy. This will be especially important given that perfectly anticipating and preventing all possible privacy problems (whether through blocking tools or careful engineering of web APIs) has proved infeasible. To enable such oversight, we plan to make all of our data publicly available (OpenWPM is already open-source). We expect that measurement will be useful to developers of privacy tools, to regulators and policy makers, journalists, and many others.

2.   BACKGROUND AND RELATED WORK

Background: third-party online tracking. As users browse and interact with websites, they are observed by both "first parties," which are the sites the user visits directly, and "third parties" which are typically hidden trackers such as ad networks embedded on most web pages. Third parties can obtain users' browsing histories through a combination of cookies and other tracking technologies that allow them to uniquely identify users, and the "referer" header that tells the third party which first-party site the user is currently visiting. Other sensitive information such as email addresses may also be leaked to third parties via the referer header.

Web privacy measurement platforms.
The closest comparisons to OpenWPM are other open web privacy measurement platforms, which we now review. We consider a tool to be a platform if is is publicly available and there is some generality to the types of studies that can be performed using it. In some cases, OpenWPM has directly built upon existing platforms, which we make explicit note of.

FPDetective is the most similar platform to OpenWPM. FPDetective uses a hybrid PhantomJS and Chromium based automation infrastructure [2], with both native browser code and a proxy for instrumentation. In the published study, the platform was used for the detection and analysis of fingerprinters, and much of the included instrumentation was built to support that. The platform allows researchers to conduct additional experiments by replacing a script which is executed with each page visit, which the authors state can be easily extended for non-fingerprinting studies.

OpenWPM differs in several ways from FPDetective: (1) it supports both stateful and stateless measurements, whereas FPDetective only supports stateless (2) it includes generic instrumentation for both stateless and stateful tracking, enabling a wider range of privacy studies without additional changes to the infrastructure (3) none of the included instru-

mentation requires native browser code, making it easier to upgrade to new or different versions of the browser, and (4) OpenWPM uses a high-level command-based architecture, which supports command re-use between studies.

Chameleon Crawler is a Chromium based crawler that utilizes the Chameleon[3] browser extension for detecting browser fingerprinting. Chameleon Crawler uses similar automation components, but supports a subset of OpenWPM's instrumentation.

FourthParty is a Firefox plug-in for instrumenting the browser and does not handle automation [23]. OpenWPM has incorporated and expanded upon nearly all of FourthParty's instrumentation (Section 3).

WebXray is a PhantomJS based tool for measuring HTTP traffic [22]. It has been used to study third-party inclusions on the top 1 million sites, but as we show in Section 3.3, measurements with a stripped-down browser have the potential to miss a large number of resource loads.

TrackingObserver is a Chrome extension that detects tracking and exposes APIs for extending its functionality such as measurement and blocking [35].

XRay [21] and *AdFisher* [9] are tools for running automated personalization detection experiments. AdFisher builds on similar technologies as OpenWPM (Selenium, xvfb), but is not intended for tracking measurements.

Common Crawl[4] uses an Apache Nutch based crawler. The Common Crawl dataset is the largest publicly available web crawl[5], with billions of page visits. However, the crawler used does not execute Javascript or other dynamic content during a page visit. Privacy studies which use the dataset [36] will miss dynamically loaded content, which includes many advertising resources.

Previous findings. Krishnarmurthy and Wills [19] provide much of the early insight into web tracking, showing the growth of the largest third-party organizations from 10% to 20-60% of top sites between 2005 and 2008. In the following years, studies show a continual increase in third-party tracking and in the diversity of tracking techniques [23, 35, 16, 2, 1, 4]. Fruchter et al. studied geographic variations in tracking [15]. More recently, Libert studied third-party HTTP requests on the top 1 million sites [22], providing view of tracking across the web. In this study, Libert showed that Google can track users across nearly 80% of sites through its various third-party domains.

Web tracking has expanded from simple HTTP cookies to include more persistent tracking techniques. Soltani et al. first examined the use of flash cookies to "respawn" or re-instantiate HTTP cookies [39], and Ayenson et al. showed how sites were using cache E-Tags and HTML5 localStorage for the same purpose [6]. Follow up studies show the technique is still used for tracking [35, 24, 1].

Device fingerprinting is a persistent tracking technique which does not require a tracker to set any state in the user's browser. Instead, trackers attempt to identify users by a combination of the device's properties. Within samples of over 100,000 browsers, 80-90% of desktop and 81% of mobile device fingerprints are unique [10, 20]. New fingerprinting techniques are continually discovered [25, 31, 14], and are

---

[3]https://github.com/ghostwords/chameleon

[4]https://commoncrawl.org

[5]https://aws.amazon.com/public-data-sets/common-crawl/

subsequently used to track users on the web [29, 2, 1]. In Section 6.1 we present several new fingerprinting techniques discovered during our measurements.

Web security measurement. Web security studies often use similar methods as web privacy measurement, and the boundary is not always clear. Yue and Wang modified the Firefox browser source code in order to perform a measurement of insecure Javascript implementations on the web [49]. Headless browsers have been used in many web security measurements, for example: to measure the amount of third-party Javascript inclusions across many popular sites and the vulnerabilities that arise from how the script is embedded [28], to measure the presence of security seals on the top 1 million sites [46], and to study stand-alone password generators and meters on the web [44]. Several studies have used Selenium-based frameworks, including: to measure and categorize malicious advertisements displayed while browsing popular sites [50], to measure the presence of malware and other vulnerabilities on live streaming websites [33], to study HSTS deployment [17], to measure ad-injecting browser extensions [48], and to emulate users browsing malicious web shells with the goal of detecting client-side homephoning [40]. Other studies have analyzed Flash and Javascript elements of webpages to measure security vulnerabilities and error-prone implementations [30, 45].

3.   MEASUREMENT PLATFORM

An infrastructure for automated web privacy measurement has three components: simulating users, recording observations (response metadata, cookies, behavior of scripts, etc.), and analysis. We set out to build a platform that can automate the first two components and can ease the researcher's analysis task. We sought to make OpenWPM general, modular, and scalable enough to support essentially any privacy measurement.

OpenWPM is open source and has already been used for measurement by several published studies. Section 3.4 in the supplementary materials examines the advanced features used by each study. In this paper we present, for the first time, the design and evaluation of the platform and highlight its strengths through several new measurements.

3.1   Design Motivations

OpenWPM builds on similar technologies as many previous platforms, but has several key design differences to support modular, comprehensive, and maintainable measurement. Our platform supports stateful measurements while FPDetective [2] does not. Stateful measurements are important for studying the tracking ecosystem. Ad auctions may vary based on cookie data. A stateless browser always appears to be a new user, which skews cookie syncing measurements. In addition to cookie syncing studied in this paper, stateful measurements have allowed our platform to be used to study cookie respawning [1] and replicate realistic user profiles [12].

Many past platforms rely on native instrumentation code [27, 38, 2], which have a high maintenance cost and, in some cases a high cost-per-API monitored. In our platform, the cost of monitoring new APIs is minimal (Section 3.3) and APIs can be enabled or disabled in the add-on without recompiling the browser or rendering engine. This allows us to monitor a larger number of APIs. Native codebase changes in other platforms require constant merges as the upstream
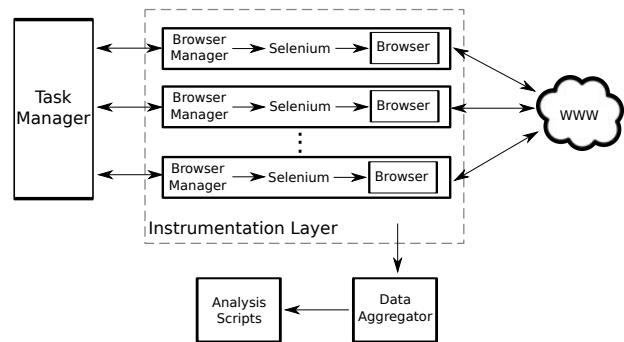
Figure 1: High-level overview of OpenWPM
The task manager monitors browser managers, which convert high-level commands into automated browser actions. The data aggregator receives and pre-processes data from instrumentation.

codebase evolves and complete rewrites to support alternative browsers.

3.2   Design and Implementation

We divided our browser automation and data collection infrastructure into three main modules: *browser managers* which act as an abstraction layer for automating individual browser instances, a user-facing *task manager* which serves to distribute commands to browser managers, and a *data aggregator*, which acts as an abstraction layer for browser instrumentation. The researcher interacts with the task manager via an extensible, high-level, domain-specific language for crawling and controlling the browser instance. The entire platform is built using Python and Python libraries.

Browser driver: Providing realism and support for web technologies. We considered a variety of choices to *drive* measurements, i.e., to instruct the browser to visit a set of pages (and possibly to perform a set of actions on each). The two main categories to choose from are lightweight browsers like PhantomJS (an implementation of WebKit), and full-fledged browsers like Firefox and Chrome. We chose to use Selenium, a cross-platform web driver for Firefox, Chrome, Internet Explorer, and PhantomJS. We currently use Selenium to drive Firefox, but Selenium's support for multiple browsers makes it easy to transition to others in the future.

By using a consumer browser, all technologies that a typical user would have access to (e.g., HTML5 storage options, Adobe Flash) are also supported by measurement instances. The alternative, PhantomJS, does not support WebGL, HTML5 Audio and Video, CSS 3-D, and browser plugins (like Flash), making it impossible to run measurements on the use of these technologies [32].

In retrospect this has proved to be a sound choice. Without full support for new web technologies we would not have been able to discover and measure the use of the `Audio-Context` API for device fingerprinting as discussed in Section 6.4.

Finally the use of real browsers also allows us to test the effects of consumer browser extensions. We support running measurements with extensions such as Ghostery and HTTPS Everywhere as well as enabling Firefox privacy settings such third-party cookie blocking and the new Tracking Protection feature. New extensions can easily be supported with only a few extra lines of code (Section 3.3). See Sec-

tion 5.3 and Section 5.5 for analyses of measurements run with these browser settings.

Browser managers: Providing stability. During the course of a long measurement, a variety of unpredictable events such as page timeouts or browser crashes could halt the measurement's progress or cause data loss or corruption. A key disadvantage of Selenium is that it frequently hangs indefinitely due to its blocking API [37], as it was designed to be a tool for webmasters to test their own sites rather than an engine for large-scale measurements. Browser managers provide an abstraction layer around Selenium, isolating it from the rest of the components.

Each browser manager instantiates a Selenium instance with a specified configuration of preferences, such as blocking third-party cookies. It is responsible for converting high-level platform commands (e.g. visiting a site) into specific Selenium subroutines. It encapsulates per-browser state, enabling recovery from browser failures. To isolate failures, each browser manager runs as a separate process.

We support launching measurement instances in a "headless" container, by using the pyvirtualdisplay library to interface with Xvfb, which draws the graphical interface of the browser to a virtual frame buffer.

Task manager: Providing scalability and abstraction. The task manager provides a scriptable command-line interface for controlling multiple browsers simultaneously. Commands can be distributed to browsers either synchronized or first-come-first-serve. Each command is launched in a per-browser command execution thread.

The command-execution thread handles errors in its corresponding browser manager automatically. If the browser manager crashes, times out, or exceeds memory limits, the thread enters a crash recovery routine. In this routine, the manager archives the current browser profile, kills all current processes, and loads the archive (which includes cookies and history) into a fresh browser with the same configuration.

Data Aggregator: Providing repeatability. Repeatability can be achieved logging data in a standardized format, so research groups can easily share scripts and data. We aggregate data from all instrumentation components in a central and structured location. The data aggregator receives data during the measurement, manipulates it as necessary, and saves it on disk keyed back to a specific page visit and browser. The aggregator exists within its own process, and is accessed through a socket interface which can easily be connected to from any number of browser managers or instrumentation processes.

We currently support two data aggregators: a structured SQLite aggregator for storing relational data and a LevelDB aggregator for storing compressed web content. The SQLite aggregator stores the majority of the measurement data, including data from both the proxy and the extension (described below). The LevelDB aggregator is designed to store de-duplicated web content, such as Javascript or HTML files. The aggregator checks if a hash of the content is present in the database, and if not compresses the content and adds it to the database.

Instrumentation: Supporting comprehensive and reusable measurement. We provide the researcher with data access at several points: (1) raw data on disk, (2) at the network level with an HTTP proxy, and (3) at the Javascript level with a Firefox extension. This provides nearly full coverage of a browser's interaction with the web and the system. Each level of instrumentation keys data with the top level site being visited and the current browser id, making it possible to combine measurement data from multiple instrumentation sources for each page visit.

Disk Access — We include instrumentation that collects changes to Flash LSOs and the Firefox cookie database after each page visit. This allows a researcher to determine which domains are setting Flash cookies, and to record access to cookies in the absence of other instrumentation

HTTP Data — After examining several Python HTTP proxies, we chose to use Mitmproxy[6] to record all HTTP Request and Response headers. We generate and load a certificate into Firefox to capture HTTPS data alongside HTTP.

Additionally, we use the HTTP proxy to dump the content of any Javascript file requested during a page visit. We use both `Content-Type` and file extension checking to detect scripts in the proxy. Once detected, a script is decompressed (if necessary) and hashed. The hash and content are sent to the LevelDBAggregator for de-duplication.

Javascript Access — We provide the researcher with a Javascript interface to pages visited through a Firefox extension. Our extension expands on the work of Fourthparty [23]. In particular, we utilize Fourthparty's Javascript instrumentation, which defines custom getters and setters on the `window.navigator` and `window.screen` interfaces[7]. We updated and extended this functionality to record access to the prototypes of the `Storage`, `HTMLCanvasElement`, `CanvasRenderingContext2D`, `RTCPeerConntection`, `AudioContext` objects, as well as the prototypes of several children of `AudioNode`. This records the setting and getting of all object properties and calls of all object methods for any object built from these prototypes. Alongside this, we record the new property values set and the arguments to all method calls. Everything is logged directly to the SQLite aggregator

In addition to recording access to instrumented objects, we record the URL of the script responsible for the property or method access. To do so, we throw an Error and parse the stack trace after each call or property intercept. This method is successful for 99.9% of Javascript files we encountered, and even works for Javascript files which have been minified or obfuscated with `eval`. A minor limitation is that the function calls of a script which gets passed into the `eval` method of a second script will have their URL labeled as the second script. This method is adapted with minor modifications from the Privacy Badger Firefox Extension[8].

In an adversarial situation, a script could disable our instrumentation before fingerprinting a user by overriding access to getters and setters for each instrumented object. However, this would be detectable since we would observe access to the `define{G,S}etter` or `lookup{G,S}etter` methods for the object in question and could investigate the cause. In our 1 million site measurement, we only observe script access to getters or setters for `HTMLCanvasElement` and `CanvasRenderingContext2D` interfaces. All of these are benign accesses from 47 scripts total, with the majority related to an HTML canvas graphics library.

---

[6]https://mitmproxy.org/

[7]In the latest public version of Fourthparty (May 2015), this instrumentation is not functional due to API changes.

[8]https://github.com/EFForg/privacybadgerfirefox

Study	Year	Browser automation	Stateful crawls	Persistent profiles	Fine-grained profiles	Advanced plugin support	Automated login	Detect tracking cookies	Monitor state changes	Javascript Instrumentation	Content extraction
Persistent tracking mechanisms [1]	2014	●	●	●	●	●		●	●		
FB Connect login permissions [34]	2014	●					●				○
Surveillance implications of web tracking [12]	2015	●	●			●		●			
HSTS and key pinning misconfigurations [17]	2015	●	●			●	○				●
The Web Privacy Census [4]	2015	●	●			●			●		
Geographic Variations in Tracking [15]	2015	●				●					
Analysis of Malicious Web Shells [40]	2016	●									
This study (Sections 5 & 6)	2016	●	●	●	●	●		●	●	●	

Table 1: Seven published studies which utilize our Platform.
An unfilled circle indicates that the feature was useful but application-specific programming or manual effort was still required.

3.3   Evaluation

Stability. We tested the stability of vanilla Selenium without our infrastructure in a variety of settings. The best average we were able to obtain was roughly 800 pages without a freeze or crash. Even in small-scale studies, the lack of recovery led to loss or corruption of measurement data. Using the isolation provided by our browser manager and task manager, we recover from all browser crashes and have observed no data corruption during stateful measurements of 100,000 sites. During the course of our stateless 1 million site measurement in January 2016 (Section 5), we observe over 90 million requests and nearly 300 million Javascript calls. A single instrumented browser can visit around 3500 sites per day, requiring no manual interaction during that time. The scale and speed of the overall measurement depends on the hardware used and the measurement configuration (See "Resource Usage" below).

Completeness. OpenWPM reproduces a human user's web browsing experience since it uses a full-fledged browser. However, researchers have used stripped-down browsers such as PhantomJS for studies, trading off fidelity for speed.

To test the importance of using a full-fledged browser, we examined the differences between OpenWPM and PhantomJS (version 2.1.1) on the top 100 Alexa sites. We averaged our results over 6 measurements of each site with each tool. Both tools were configured with a time-out of 10 seconds and we excluded a small number of sites that didn't complete loading. Unsurprisingly, PhantomJS does not load Flash, HTML5 Video, or HTML5 Audio objects (which it does not support); OpenWPM loads nearly 300 instances of those across all sites. More interestingly, PhantomJS loads about 30% fewer HTML files, and about 50% fewer resources with plain text and stream content types. Upon further examination, one major reason for this is that many sites don't serve ads to PhantomJS. This makes tracking measurements using PhantomJS problematic.

We also tested PhantomJS with the user-agent string spoofed to look like Firefox, so as to try to prevent sites from treating PhantomJS differently. Here the differences were less extreme, but still present (10% fewer requests of html resources, 15% for plain text, and 30% for stream). However, several sites (such as `dropbox.com`) seem to break when PhantomJS presents the incorrect user-agent string. This

is because sites may expect certain capabilities that PhantomJS does not have or may attempt to access APIs using Firefox-specific names. One site, `weibo.com`, redirected PhantomJS (with either user-agent string) to an entirely different landing page than OpenWPM. These findings support our view that OpenWPM enables significantly more complete and realistic web and tracking measurement than stripped-down browsers.

Resource usage. When using the headless configuration, we are able to run up to 10 stateful browser instances on an Amazon EC2 "c4.2xlarge" virtual machine[9]. This virtual machine costs around $300 per month using price estimates from May 2016. Due to Firefox's memory consumption, stateful parallel measurements are memory-limited while stateless parallel measurements are typically CPU-limited and can support a higher number of instances. On the same machine we can run 20 browser instances in parallel if the browser state is cleared after each page load.

Generality. The platform minimizes code duplication both across studies and across configurations of a specific study. For example, the Javascript monitoring instrumentation is about 340 lines of Javascript code. Each additional API monitored takes only a few additional lines of code. The instrumentation necessary to measure canvas fingerprinting (Section 6.1) is three additional lines of code, while the WebRTC measurement (Section 6.3) is just a single line of code.

Similarly, the code to add support for new extensions or privacy settings is relatively low: 7 lines of code were required to support Ghostery, 8 lines of code to support HTTPS Everywhere, and 7 lines of codes to control Firefox's cookie blocking policy.

Even measurements themselves require very little additional code on top of the platform. Each configuration listed in Table 2 requires between 70 and 108 lines of code. By comparison, the core infrastructure code and included instrumentation is over 4000 lines of code, showing that the platform saves a significant amount of engineering effort.

3.4   Applications of OpenWPM

Seven academic studies have been published in journals, conferences, and workshops, utilizing OpenWPM to perform

---

[9]https://aws.amazon.com/ec2/instance-types/

a variety of web privacy and security measurements. Table 1 summarizes the advanced features of the platform each research group utilized in their measurements.

In addition to *browser automation* and HTTP data dumps, the platform has several advanced capabilities used by both our own measurements and those in other groups. Measurements can keep state, such as cookies and localStorage, within each session via *stateful measurements*, or persist this state across sessions with *persistent profiles*. Persisting state across measurements has been used to measure cookie respawning [1] and to provide seed profiles for larger measurements (Section 5). In general, stateful measurements are useful to replicate the cookie profile of a real user for tracking [4, 12] and cookie syncing analysis [1] (Section 5.6). In addition to recording state, the platform can *detect tracking cookies*.

The platform also provides programmatic control over individual components of this state such as Flash cookies through *fine-grained profiles* as well as plug-ins via *advanced plug-in support*. Applications built on top of the platform can *monitor state changes* on disk to record access to Flash cookies and browser state. These features are useful in studies which wish to simulate the experience of users with Flash enabled [4, 15] or examine cookie respawning with Flash [1].

Beyond just monitoring and manipulating state, the platform provides the ability to capture any Javascript API call with the included *Javascript instrumentation*. This is used to measure device fingerprinting (Section 6).

Finally, the platform also has a limited ability to extract content from web pages through the *content extraction* module, and a limited ability to automatically log into websites using the Facebook Connect *automated login* capability. Logging in with Facebook has been used to study login permissions [34].

4. WEB CENSUS METHODOLOGY

We run measurements on the homepages of the top 1 million sites to provide a comprehensive view of web tracking and web privacy. These measurements provide updated metrics on the use of tracking and fingerprinting technologies, allowing us to shine a light onto the practices of third parties and trackers across a large portion of the web. We also explore the effectiveness of consumer privacy tools at giving users control over their online privacy.

Measurement Configuration. We run our measurements on a "c4.2xlarge" Amazon EC2 instance, which currently allocates 8 vCPUs and 15 GiB of memory per machine. With this configuration we are able to run 20 browser instances in parallel. All measurements collect HTTP Requests and Responses, Javascript calls, and Javascript files using the instrumentation detailed in Section 3. Table 2 summarizes the measurement instance configurations. The data used in this paper were collected during January 2016.

All of our measurements use the Alexa top 1 million site list (http://www.alexa.com), which ranks sites based on their global popularity with Alexa Toolbar users. Before each measurement, OpenWPM retrieves an updated copy of the list. When a measurement configuration calls for less than 1 million sites, we simply truncate the list as necessary. For eash site, the browser will visit the homepage and wait until the site has finished loading or until the 90 second timeout is reached. The browser does not interact with the site or visit any other pages within the site. If there is a timeout we kill the process and restart the browser for the next page visit, as described in Section 3.2.

Stateful measurements. To obtain a complete picture of tracking we must carry out stateful measurements in addition to stateless ones. Stateful measurements do not clear the browser's profile between page visits, meaning cookie and other browser storage persist from site to site. For some measurements the difference is not material, but for others, such as cookie syncing (Section 5.6), it is essential.

Making stateful measurements is fundamentally at odds with parallelism. But a serial measurement of 1,000,000 sites (or even 100,000 sites) would take unacceptably long. So we make a compromise: we first build a *seed profile* which visits the top 10,000 sites in a serial fashion, and we save the resulting state.

To scale to a larger measurement, the seed profile is loaded into multiple browser instances running in parallel. With this approach, we can approximately simulate visiting each website serially. For our 100,000 site stateless measurement, we used the "ID Detection 2" browser profile as a seed profile.

This method is not without limitations. For example third parties which don't appear in the top sites if the seed profile will have different cookies set in each of the parallel instances. If these parties are also involved in cookie syncing, the partners that sync with them (and appear in the seed profile) will each receive multiple IDs for each one of their own. This presents a trade-off between the size the seed profile and the number of third parties missed by the profile. We find that a seed profile which has visited the top 10,000 sites will have communicated with 76% of all third-party domains present on more than 5 of the top 100,000 sites.

Handling errors. In presenting our results we only consider sites that loaded successfully. For example, for the 1 Million site measurement, we present statistics for 917,261 sites. The majority of errors are due to the site failing to return a response, primarily due to DNS lookup failures. Other causes of errors are sites returning a non-2XX HTTP status code on the landing page, such as a 404 (Not Found) or a 500 (Internal Server Error).

Detecting ID cookies. Detecting cookies that store unique user identifiers is a key task that enables many of the results that we report in Section 5. We build on the methods used in previous studies [1, 12]. Browsers store cookies in a structured key-value format, allowing sites to provide both a *name string* and *value string*. Many sites further structure the value string of a single cookie to include a set of named parameters. We parse each cookie value string assuming the format:

$$(\text{name}_1 =)\text{value}_1|...|(\text{name}_N =)\text{value}_N$$

where | represents any character except a-zA-Z0-9_-=. We determine a (cookie-name, parameter-name, parameter-value) tuple to be an ID cookie if it meets the following criteria: (1) the cookie has an expiration date over 90 days in the future (2) $8 \leq$ length(parameter-value) ≤ 100, (3) the parameter-value remains the same throughout the measurement, (4) the parameter-value is different between machines and has a similarity less than 66% according to the Ratcliff-Obershelp algorithm [7]. For the last step, we run two synchronized measurements (see Table 2) on separate machines and compare the resulting cookies, as in previous studies.

What makes a tracker? Every third party is *potentially*

Configuration	# Sites	# Success	Timeout %	Flash Enabled	Stateful	Parallel	HTTP Data	Javascript Files	Javascript Calls	Disk Scans	Time to Crawl
Default Stateless	1 Million	917,261	10.58%			●	●	●	●		14 days
Default Stateful	100,000	94,144	8.23%		○	●	●	●	●		3.5 days
Ghostery	55,000	50,023	5.31%			●	●	●	●		0.7 days
Block TP Cookies	55,000	53,688	12.41%			●	●	●	●		0.8 days
HTTPS Everywhere	55,000	53,705	14.77%			●	●	●	●		1 day
ID Detection 1*	10,000	9,707	6.81%	●	●		●	●	●	●	2.9 days
ID Detection 2*	10,000	9,702	6.73%	●	●		●	●	●	●	2.9 days

Table 2: Census measurement configurations.
An unfilled circle indicates that a seed profile of length 10,000 was loaded into each browser instance in a parallel measurement. "# Success" indicates the number of sites that were reachable and returned a response. A Timeout is a request which fails to completely load in 90 seconds. *Indicates that the measurements were run synchronously on different virtual machines.

a tracker, but for many of our results we need a more conservative definition. We use two popular *tracking-protection lists* for this purpose: EasyList and EasyPrivacy. Including EasyList allows us to classify advertising related trackers, while EasyPrivacy detects non-advertising related trackers. The two lists consist of regular expressions and URL substrings which are matched against resource loads to determine if a request should be blocked.

Alternative tracking-protection lists exist, such as the list built into the Ghostery browser extension and the domain-based list provided by Disconnect[10]. Although we don't use these lists to classify trackers directly, we evaluate their performance in several sections.

Note that we are not simply classifying domains as trackers or non-trackers, but rather classify each instance of a third party on a particular website as a tracking or non-tracking context. We consider a domain to be in the tracking context if a consumer privacy tool would have blocked that resource. Resource loads which wouldn't have been blocked by these extensions are considered non-tracking.

While there is agreement between the extensions utilizing these lists, we emphasize that they are far from perfect. They contain false positives and especially false negatives. That is, they miss many trackers — new ones in particular. Indeed, much of the impetus for OpenWPM and our measurements comes from the limitations of manually identifying trackers. Thus, tracking-protection lists should be considered an underestimate of the set of trackers, just as considering all third parties to be trackers is an overestimate.

Limitations. The analysis presented in this paper has several methodological and measurement limitations. Our platform did not interact with sites in ways a real user might; we did not log into sites nor did we carry out actions such as scrolling or clicking links during our visit. While we have performed deeper crawls of sites (and plan to make this data publicly available), the analyses presented in the paper pertain only to homepages.

For comparison, we include a preliminary analysis of a crawl which visits 4 internal pages in addition to the homepage of the top 10,000 sites. The analyses presented in this paper should be considered a lower bound on the amount of tracking a user will experience in the wild. In particular, the average number of third parties per site increases from 22 to 34. The 20 most popular third parties embedded on the

---

[10]https://disconnect.me/trackerprotection

homepages of sites are found on 6% to 57% more sites when internal page loads are considered. Similarly, fingerprinting scripts found in Section 6 were observed on more sites. Canvas fingerprinting increased from 4% to 7% of the top sites while canvas-based font fingerprinting increased from 2% to 2.5%. An increase in trackers is expected as each additional page visit within a site will cycle through new dynamic content that may load a different set of third parties. Additionally, sites may not embed all third-party content into their homepages.

The measurements presented in this paper were collected from an EC2 instance in Amazon's US East region. It is possible that some sites would respond differently to our measurement instance than to a real user browsing from residential or commercial internet connection. Fruchter, et al. [15] use OpenWPM to measure the variation in tracking due to geographic differences. They found no evidence of tracking differences caused by the origin of the measurement instance.

Although OpenWPM's instrumentation measures a diverse set of tracking techniques, we do not provide a complete analysis of all known techniques. Notably absent from our analysis are non-canvas-based font fingerprinting [2], navigator and plugin fingerprinting [10, 23], and cookie respawning [39, 6]. Several of these javascript-based techniques are currently supported by OpenWPM, have been measured with OpenWPM in past research [1], and others can be easily added (Section 3.3). Non-Javascript techniques, such as font fingerprinting with Adobe Flash, would require additional specialized instrumentation.

Finally, for readers interested in further details or in reproducing our work, we provide further methodological details in the full version of this paper: what constitutes distinct domains, how to detect the landing page of a site using the data collected by OpenWPM, how we detect cookie syncing, and why obfuscation of Javascript doesn't affect our ability to detect fingerprinting.

5. RESULTS OF 1-MILLION SITE CENSUS

5.1 The long but thin tail of online tracking

During our January 2016 measurement of the Top 1 million sites, our tool made over 90 million requests, assembling the largest dataset on web tracking to our knowledge.

Our large scale allows us to answer a rather basic question: how many third parties are there? In short, a lot: the

total number of third parties present on at least two first parties is over 81,000.

What is more surprising is that the prevalence of third parties quickly drops off: only 123 of these 81,000 are present on more than 1% of sites. This suggests that the number of third parties that a regular user will encounter on a daily basis is relatively small. The effect is accentuated when we consider that different third parties may be owned by the same entity. All of the top 5 third parties, as well as 12 of the top 20, are Google-owned domains. In fact, *Google, Facebook, Twitter, and AdNexus are the only third-party entities present on more than 10% of sites.*

We can expand on this by analyzing the top third-party *organizations*, many of which consist of multiple entities. As an example, Facebook and Liverail are separate entities but Liverail is owned by Facebook. We use the domain-to-organization mappings provided by Libert [22] and Disconnect. With these mappings considered, Google, Facebook, Twitter, Amazon, AdNexus, and Oracle are the third-party organizations present on more than 10% of sites. In comparison to Libert's [22] 2014 findings, Akamai and ComScore fall significantly in market share to just 2.4% and 6.6% of sites. Oracle joins the top third parties by purchasing BlueKai and AddThis, showing that acquisitions can quickly change the tracking landscape.

Further, if we use the definition of tracking based on tracking-protection lists, as defined in Section 4, then trackers are even less prevalent. This is clear from Figure 2, which shows the prevalence of the top third parties (a) in any context and (b) only in tracking contexts. Note the absence or reduction of content-delivery domains such as gstatic.com, fbcdn.net, and googleusercontent.com.

Larger entities may be easier to regulate by public-relations pressure and the possibility of legal or enforcement actions, an outcome we have seen in past studies [1, 6, 24].
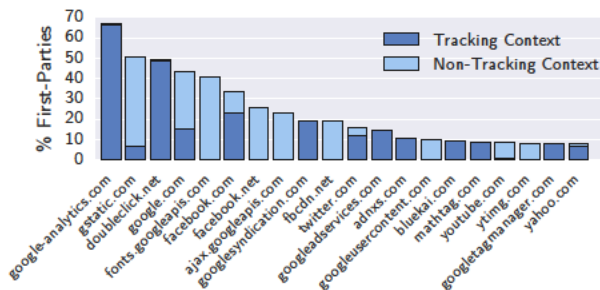
Figure 2: Top third parties on the top 1 million sites. Not all instances of third parties are classified as tracking by our methodology, and in fact the same third party can be classified differently depending on the context. (Section 4).

5.2   Prominence: a third party ranking metric

In Section 5.1 we ranked third parties by the number of first party sites they appear on. This simple count is a good first approximation, but it has two related drawbacks. A major third party that's present on (say) 90 of the top 100 sites would have a low score if its prevalence drops off outside the top 100 sites. A related problem is that the rank can be sensitive to the number of websites visited in the measurement. Thus different studies may rank third parties differently.

We also lack a good way to compare third parties (and especially trackers) over time, both individually and in ag-
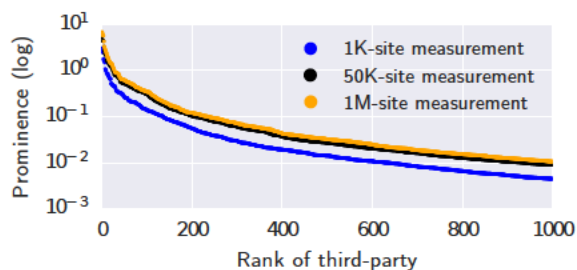
Figure 3: Prominence of third party as a function of prominence rank. We posit that the curve for the 1M-site measurement (which can be approximated by a 50k-site measurement) presents a useful aggregate picture of tracking.

gregate. Some studies have measured the total number of cookies [4], but we argue that this is a misleading metric, since cookies may not have anything to do with tracking.

To avoid these problems, we propose a principled metric. We start from a model of aggregate browsing behavior. There is some research suggesting that the website traffic follows a power law distribution, with the frequency of visits to the Nth ranked website being proportional to $\frac{1}{N}$ [3, 18]. The exact relationship is not important to us; any formula for traffic can be plugged into our prominence metric below.

Definition:.

$$\text{Prominence}(t) = \Sigma_{edge(s,t)=1} \frac{1}{rank(s)}$$

where $edge(s,t)$ indicates whether third party t is present on site s. This simple formula measures the frequency with which an "average" user browsing according to the power-law model will encounter any given third party.

The most important property of prominence is that it de-emphasizes obscure sites, and hence can be adequately approximated by relatively small-scale measurements, as shown in Figure 3. We propose that prominence is the right metric for:

1. Comparing third parties and identifying the top third parties. We present the list of top third parties by prominence in the full version of this paper. Prominence ranking produces interesting differences compared to ranking by a simple prevalence count. For example, Content-Distribution Networks become less prominent compared to other types of third parties.
2. Measuring the effect of tracking-protection tools, as we do in Section 5.5.
3. Analyzing the evolution of the tracking ecosystem over time and comparing between studies. The robustness of the *rank-prominence curve* (Figure 3) makes it ideally suited for these purposes.

5.3   Third parties impede HTTPS adoption

Table 3 shows the number of first-party sites that support HTTPS and the number that are HTTPS-only. Our results reveal that HTTPS adoption remains rather low despite well-publicized efforts [11]. Publishers have claimed that a major roadblock to adoption is the need to move all embedded third parties and trackers to HTTPS to avoid mixed-content errors [41, 47].

Mixed-content errors occur when HTTP sub-resources are loaded on a secure site. This poses a security problem, leading to browsers to block the resource load or warn the user depending on the content loaded [26]. *Passive* mixed content, that is, non-executable resources loaded over HTTP,

	55K Sites	1M Sites
HTTP Only	82.9%	X
HTTPS Only	14.2%	8.6%
HTTPS Opt.	2.9%	X

Table 3: First party HTTPS support on the top 55K and top 1M sites. "HTTP Only" is defined as sites which fail to upgrade when HTTPS Everywhere is enabled. 'HTTPS Only" are sites which always redirect to HTTPS. "HTTPS Optional" are sites which provide an option to upgrade, but only do so when HTTPS Everywhere is enabled. We carried out HTTPS-everywhere-enabled measurement for only 55,000 sites, hence the X's.

HTTPS Support	Percent	Prominence weighted %
HTTP Only	54%	5%
HTTPS Only	5%	1%
Both	41%	94%

Table 4: Third party HTTPS support. "HTTP Only" is defined as domains from which resources are only requested over HTTP across all sites on our 1M site measurement. 'HTTPS Only" are domains from which resources are only requested over HTTPS. "Both" are domains which have resources requested over both HTTP and HTTPS. Results are limited to third parties embedded on at least 10 first-party sites.

cause the browser to display an insecure warning to the user but still load the content. *Active* mixed content is a far more serious security vulnerability and is blocked outright by modern browsers; it is not reflected in our measurements.

Third-party support for HTTPS. To test the hypothesis that third parties impede HTTPS adoption, we first characterize the HTTPS support of each third party. If a third party appears on at least 10 sites and is loaded over HTTPS on all of them, we say that it is HTTPS-only. If it is loaded over HTTPS on some but not all of the sites, we say that it supports HTTPS. If it is loaded over HTTP on all of them, we say that it is HTTP-only. If it appears on less than 10 sites, we do not have enough confidence to make a determination.

Table 4 summarizes the HTTPS support of third party domains. A large number of third-party domains are HTTP-only (54%). However, when we weight third parties by prominence, only 5% are HTTP-only. In contrast, 94% of prominence-weighted third parties support both HTTP and HTTPS. This supports our thesis that consolidation of the third-party ecosystem is a plus for security and privacy.

Impact of third-parties. We find that a significant fraction of HTTP-default sites (26%) embed resources from third-parties which do not support HTTPS. These sites would be unable to upgrade to HTTPS without browsers displaying mixed content errors to their users, the majority of which (92%) would contain active content which would be blocked.

Similarly, of the approximately 78,000 first-party sites that are HTTPS-only, around 6,000 (7.75%) load with mixed passive content warnings. However, only 11% of these warnings (around 650) are caused by HTTP-only third parties, suggesting that many domains may be able to mitigate these warnings by ensuring all resources are being loaded over HTTPS when available. We examined the causes of mixed content on these sites, summarized in Table 5. The majority are caused by third parties, rather than the site's own content, with a surprising 27% caused solely by trackers.

Class	Top 1M % FP	Top 55k % FP
Own	25.4%	24.9%
Favicon	2.1%	2.6%
Tracking	10.4%	20.1%
CDN	1.6%	2.6%
Non-tracking	44.9%	35.4%
Multiple causes	15.6%	6.3%

Table 5: A breakdown of causes of passive mixed-content warnings on the top 1M sites and on the top 55k sites. "Non-tracking" represents third-party content not classified as a tracker or a CDN.
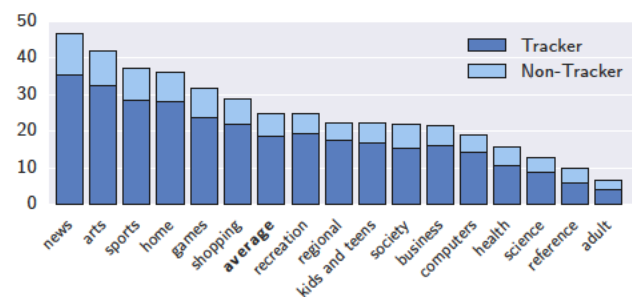
Figure 4: Average # of third parties in each Alexa category.

5.4   News sites have the most trackers

The level of tracking on different categories of websites varies considerably — by almost an order of magnitude. To measure variation across categories, we used Alexa's lists of top 500 sites in each of 16 categories. From each list we sampled 100 sites (the lists contain some URLs that are not home pages, and we excluded those before sampling).

In Figure 4 we show the average number of third parties loaded across 100 of the top sites in each Alexa category. Third parties are classified as trackers if they would have been blocked by one of the tracking protection lists (Section 4).

Why is there so much variation? With the exception of the adult category, the sites on the low end of the spectrum are mostly sites which belong to government organizations, universities, and non-profit entities. This suggests that websites may be able to forgo advertising and tracking due to the presence of funding sources external to the web. Sites on the high end of the spectrum are largely those which provide editorial content. Since many of these sites provide articles for free, and lack an external funding source, they are pressured to monetize page views with significantly more advertising.

5.5   Does tracking protection work?

Users have two main ways to reduce their exposure to tracking: the browser's built in privacy features and extensions such as Ghostery or uBlock Origin.

Contrary to previous work questioning the effectiveness of Firefox's third-party cookie blocking [12], we do find the feature to be effective. Specifically, only 237 sites (0.4%) have any third-party cookies set during our measurement set to block all third-party cookies ("Block TP Cookies" in Table 2). Most of these are for benign reasons, such as redirecting to the U.S. version of a non-U.S. site. We did find exceptions, including 32 that contained ID cookies. For example, there are six Australian news sites that first redirect to `news.com.au` before re-directing back to the initial domain,
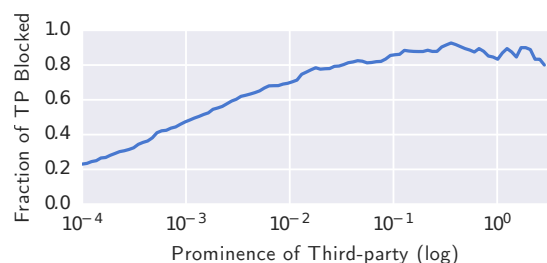
Figure 5: Fraction of third parties blocked by Ghostery as a function of the prominence of the third party. As defined earlier, a third party's prominence is the sum of the inverse ranks of the sites it appears on.

which seems to be for tracking purposes. While this type of workaround to third-party cookie blocking is not rampant, we suggest that browser vendors should closely monitor it and make changes to the blocking heuristic if necessary.

Another interesting finding is that when third-party cookie blocking was enabled, the average number of third parties per site dropped from 17.7 to 12.6. Our working hypothesis for this drop is that deprived of ID cookies, third parties curtail certain tracking-related requests such as cookie syncing (which we examine in Section 5.6).

We also tested Ghostery, and found that it is effective at reducing the number of third parties and ID cookies. The average number of third-party includes went down from 17.7 to 3.3, of which just 0.3 had third-party cookies (0.1 with IDs). We examined the prominent third parties that are not blocked and found almost all of these to be content-delivery networks like cloudflare.com or widgets like maps.google. com, which Ghostery does not try to block. So Ghostery works well at achieving its stated objectives.

However, the tool is less effective for obscure trackers (prominence < 0.1). In Section 6.6, we show that less prominent fingerprinting scripts are not blocked as frequently by blocking tools. This makes sense given that the block list is manually compiled and the developers are less likely to have encountered obscure trackers. It suggests that large-scale measurement techniques like ours will be useful for tool developers to minimize gaps in their coverage.

5.6 How common is cookie syncing?

Cookie syncing, a workaround to the Same-Origin Policy, allows different trackers to share user identifiers with each other. Besides being hard to detect, cookie syncing enables back-end server-to-server data merges hidden from public view, which makes it a privacy concern.

Our ID cookie detection methodology (Section 4) allows us to detect instances of cookie syncing. If tracker A wants to share its ID for a user with tracker B, it can do so in one of two ways: embedding the ID in the request URL to tracker B, or in the referer URL. We therefore look for instances of IDs in referer, request, and response URLs, accounting for URL encoding and other subtleties. We describe the complete details of our methodology in the full version of this paper, with an important caveat that our methodology captures both intentional and accidental ID sharing.

Most third parties are involved in cookie syncing. We run our analysis on the top 100,000 site stateful measurement. The most prolific cookie-syncing third party is `doubleclick.net` — it shares 108 different cookies with 118

other third parties (this includes both events where it is a referer and where it is a receiver).

More interestingly, we find that the vast majority of top third parties sync cookies with at least one other party: 45 of the top 50, 85 of the top 100, 157 of the top 200, and 460 of the top 1,000. This adds further evidence that cookie syncing is an under-researched privacy concern.

We also find that third parties are highly connected by synced cookies. Specifically, of the top 50 third parties that are involved in cookie syncing, the probability that a random pair will have at least one cookie in common is 85%. The corresponding probability for the top 100 is 66%.

6. FINGERPRINTING: A 1-MILLION SITE VIEW

OpenWPM significantly reduces the engineering requirement of measuring device fingerprinting, making it easy to update old measurements and discover new techniques. In this section, we demonstrate this through several new fingerprinting measurements, two of which have never been measured at scale before, to the best of our knowledge. We show how the number of sites on which font fingerprinting is used and the number of third parties using canvas fingerprinting have both increased by considerably in the past few years. We also show how WebRTC's ability to discover local IPs without user permission or interaction is used almost exclusively to track users. We analyze a new fingerprinting technique utilizing `AudioContext` found during our investigations. Finally, we discuss the use of the Battery API by two fingerprinting scripts.

Our fingerprinting measurement methodology utilizes data collected by the Javascript instrumentation described in Section 3.2. With this instrumentation, we monitor access to all built-in interfaces and objects we suspect may be used for fingerprinting. By monitoring on the interface or object level, we are able to record access to all method calls and property accesses for each interface we thought might be useful for fingerprinting. This allows us to build a detection criterion for each fingerprinting technique after a detailed analysis of example scripts.

Although our detection criteria currently have negligible low false positive rate, we recognize that this may change as new web technologies and applications emerge. However, instrumenting all properties and methods of an API provides a complete picture of each application's use of the interface, allowing our criteria to also be updated. More importantly, this allows us to replace our detection criteria with machine learning, which is an area of ongoing work (Section 7).

Rank Interval	% of First-parties		
	Canvas	Canvas Font	WebRTC
[0, 1K)	5.10%	2.50%	0.60%
[1K, 10K)	3.91%	1.98%	0.42%
[10K, 100K)	2.45%	0.86%	0.19%
[100K, 1M)	1.31%	0.25%	0.06%

Table 6: Prevalence of fingerprinting scripts on different slices of the top sites. More popular sites are more likely to have fingerprinting scripts.

6.1 Canvas Fingerprinting

Privacy threat. The HTML Canvas allows web application to draw graphics in real time, with functions to sup-

port drawing shapes, arcs, and text to a custom canvas element. In 2012 Mowery and Schacham demonstrated how the HTML Canvas could be used to fingerprint devices [25]. Differences in font rendering, smoothing, anti-aliasing, as well as other device features cause devices to draw the image differently. This allows the resulting pixels to be used as part of a device fingerprint.

Detection methodology. We build on a 2014 measurement study by Acar et.al. [1]. Since that study, the canvas API has received broader adoption for non-fingerprinting purposes, so we make several changes to reduce false positives. In our measurements we record access to nearly all of properties and methods of the `HTMLCanvasElement` interface and of the `CanvasRenderingContext2D` interface. We filter scripts according to the following criteria:

1. The canvas element's `height` and `width` properties must not be set below 16 px.[11]
2. Text must be written to canvas with least two colors or at least 10 distinct characters.
3. The script should not call the `save`, `restore`, or `addEventListener` methods of the rendering context.
4. The script extracts an image with `toDataURL` or with a single call to `getImageData` that specifies an area with a minimum size of 16px × 16px.

This heuristic is designed to filter out scripts which are unlikely to have sufficient complexity or size to act as an identifier. We manually verified the accuracy of our detection methodology by inspecting the images drawn and the source code. We found a mere 4 false positives out of 3493 scripts identified on a 1 million site measurement. Each of the 4 is only present on a single first-party.

Results. We found canvas fingerprinting on 14,371 (1.6%) sites. The vast majority (98.2%) are from third-party scripts. These scripts come from about 3,500 URLs hosted on about 400 domains. Table 7 shows the top 5 domains which serve canvas fingerprinting scripts ordered by the number of first-parties they are present on.

Domain	# First-parties
doubleverify.com	7806
lijit.com	2858
alicdn.com	904
audienceinsights.net	499
boo-box.com	303
407 others	*2719*
TOTAL	15089 (*14371 unique*)

Table 7: Canvas fingerprinting on the Alexa Top 1 Million sites. For a more complete list of scripts, see the full version of this paper.

Comparing our results with a 2014 study [1], we find three important trends. First, the most prominent trackers have by-and-large stopped using it, suggesting that the public backlash following that study was effective. Second, the overall number of domains employing it has increased considerably, indicating that knowledge of the technique has spread and that more obscure trackers are less concerned about public perception. As the technique evolves, the images used have increased in variety and complexity, as we

detail in the full version of this paper. Third, the use has shifted from behavioral tracking to fraud detection, in line with the ad industry's self-regulatory norm regarding acceptable uses of fingerprinting.

6.2   Canvas Font Fingerprinting

Privacy threat. The browser's font list is very useful for device fingerprinting [10]. The ability to recover the list of fonts through Javascript or Flash is known, and existing tools aim to protect the user against scripts that do that [29, 2]. But can fonts be enumerated using the Canvas interface? The only public discussion of the technique seems to be a Tor Browser ticket from 2014[12]. To the best of our knowledge, we are the first to measure its usage in the wild.

Detection methodology. The `CanvasRenderingContext2D` interface provides a `measureText` method, which returns several metrics pertaining to the text size (including its width) when rendered with the current font settings of the rendering context. Our criterion for detecting canvas font fingerprinting is: the script sets the `font` property to at least 50 distinct, valid values and also calls the `measureText` method at least 50 times on the same text string. We manually examined the source code of each script found this way and verified that there are zero false positives on our 1 million site measurement.

Results. We found canvas-based font fingerprinting present on 3,250 first-party sites. This represents less than 1% of sites, but as Table 6 shows, the technique is more heavily used on the top sites, reaching 2.5% of the top 1000.

The vast majority of cases (90%) are served by a single third party, mathtag.com. The number of sites with font fingerprinting represents a seven-fold increase over a 2013 study [2], although they did not consider Canvas. See the full version of this paper for a complete list of scripts.

6.3   WebRTC-based fingerprinting

Privacy threat. WebRTC is a framework for peer-to-peer Real Time Communication in the browser, and accessible via Javascript. To discover the best network path between peers, each peer collects all available candidate addresses, including addresses from the local network interfaces (such as ethernet or WiFi) and addresses from the public side of the NAT and makes them available to the web application *without explicit permission from the user*. This has led to serious privacy concerns: users behind a proxy or VPN can have their ISP's public IP address exposed [43]. We focus on a slightly different privacy concern: users behind a NAT can have their local IP address revealed, which can be used as an identifier for tracking. A detailed description of the discovery process is available in the full version of this paper.

Detection methodology. To detect WebRTC local IP discovery, we instrument the `RTCPeerConnection` interface prototype and record access to its method calls and property access. After the measurement is complete, we select the scripts which call the `createDataChannel` and `createOffer` APIs, and access the event handler `onicecandidate`[13]. We manually verified that scripts that call these

---

[11]The default canvas size is 300px × 150px.

[12]https://trac.torproject.org/projects/tor/ticket/13400

[13]Although we found it unnecessary for current scripts, instrumenting `localDescription` will cover all possible IP address retrievals.

functions are in fact retrieving candidate IP addresses, with zero false positives on 1 million sites. Next, we manually tested if such scripts are using these IPs for tracking. Specifically, we check if the code is located in a script that contains other known fingerprinting techniques, in which case we label it tracking. Otherwise, if we manually assess that the code has a clear non-tracking use, we label it non-tracking. If neither of these is the case, we label the script as 'unknown'. We emphasize that even the non-tracking scripts present a privacy concern related to leakage of private IPs.

Results. We found WebRTC being used to discover local IP addresses without user interaction on 715 sites out of the top 1 million. The vast majority of these (659) were done by third-party scripts, loaded from 99 different locations. A large majority (625) were used for tracking. The top 10 scripts accounted for 83% of usage, in line with our other observations about the small number of third parties responsible for most tracking. We provide a list of scripts in the full version of this paper.

The number of confirmed non-tracking uses of unsolicited IP candidate discovery is small, and based on our analysis, none of them is critical to the application. These results have implications for the ongoing debate on whether or not unsolicited WebRTC IP discovery should be private by default [43, 8, 42].

Classification	# Scripts	# First-parties
Tracking	57	625 (88.7%)
Non-Tracking	10	40 (5.7%)
Unknown	32	40 (5.7%)

Table 8: Summary of WebRTC local IP discovery on the top 1 million Alexa sites.

6.4   AudioContext Fingerprinting

The scale of our data gives us a new way to systematically identify new types of fingerprinting not previously reported in the literature. The key insight is that fingerprinting techniques typically aren't used in isolation but rather in conjunction with each other. So we monitor known tracking scripts and look for unusual behavior (e.g., use of new APIs) in a semi-automated fashion.

Using this approach we found several fingerprinting scripts utilizing `AudioContext` and related interfaces.

In the simplest case, a script from the company Liverail[14] checks for the existence of an `AudioContext` and `OscillatorNode` to add a single bit of information to a broader fingerprint. More sophisticated scripts process an audio signal generated with an `OscillatorNode` to fingerprint the device. This is conceptually similar to canvas fingerprinting: audio signals processed on different machines or browsers may have slight differences due to hardware or software differences between the machines, while the same combination of machine and browser will produce the same output.

Figure 6 shows one of two audio fingerprinting configurations found in three scripts. The second configuration utilizes an `AnalyserNode` to extract an FFT to build the fingerprint. Both configurations process an audio signal from an `OscillatorNode` before reading the resulting signal and hashing it to create a device audio fingerprint. Complete configuration details are available in the full version of this paper.

---

[14]https://www.liverail.com/
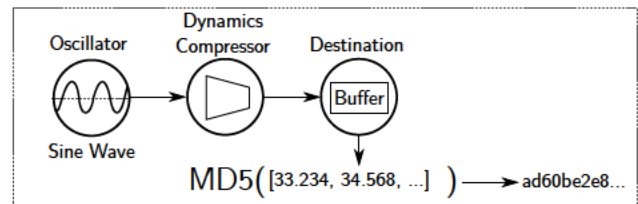
Figure 6: AudioContext node configuration used to generate a fingerprint by client.a.pxi.pub/*/main.min.js and js.ad-score.com/score.min.js in an `OfflineAudioContext`.
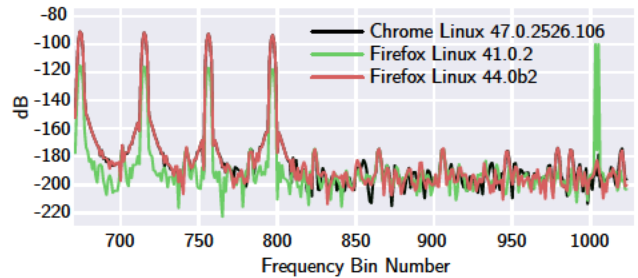
Figure 7: Visualization of processed `OscillatorNode` output from the fingerprinting script https://www.cdn-net.com/cc.js for three different browsers on the same machine. We found these values to remain constant for each browser after several checks.

We created a demonstration page based on the scripts, which attracted visitors with 18,500 distinct cookies as of this submission. These 18,500 devices hashed to a total of 713 different fingerprints. We estimate the entropy of the fingerprint at 5.4 bits based on our sample. We leave a full evaluation of the effectiveness of the technique to future work.

We find that this technique is very infrequently used as of March 2016. The most popular script is from Liverail, present on 512 sites. Other scripts were present on as few as 6 sites.

This shows that even with very low usage rates, we can successfully bootstrap off of currently known fingerprinting scripts to discover and measure new techniques.

6.5   Battery API Fingerprinting

As a second example of bootstrapping, we analyze the Battery Status API, which allows a site to query the browser for the current battery level or charging status of a host device. Olejnik et al. provide evidence that the Battery API can be used for tracking [31]. The authors show how the battery charge level and discharge time have a sufficient number of states and lifespan to be used as a short-term identifier. These status readouts can help identify users who take action to protect their privacy while already on a site. For example, the readout may remain constant when a user clears cookies, switches to private browsing mode, or opens a new browser before re-visiting the site. We discovered two fingerprinting scripts utilizing the API during our manual analysis of other fingerprinting techniques.

One script, https://go.lynxbroker.de/eat_heartbeat.js, retrieves the current charge level of the host device and combines it with several other identifying features. These features include the canvas fingerprint and the user's local IP address retrieved with WebRTC as described in Section 6.1 and Section 6.3. The second script, http://js.ad-score.com/score.min.js, queries all properties of the `BatteryManager`

1399

interface, retrieving the current charging status, the charge level, and the time remaining to discharge or recharge. As with the previous script, these features are combined with other identifying features used to fingerprint a device.

6.6 The wild west of fingerprinting scripts

In Section 5.5 we found the various tracking protection measures to be very effective at reducing third-party tracking. In Table 9 we show how blocking tools miss many of the scripts we detected throughout Section 6, particularly those using lesser-known techniques. Although blocking tools detect the majority of instances of well-known techniques, only a fraction of the total number of scripts are detected.

	Disconnect		EL + EP	
Technique	% Scripts	% Sites	% Scripts	% Sites
Canvas	17.6%	78.5%	25.1%	88.3%
Canvas Font	10.3%	97.6%	10.3%	90.6%
WebRTC	1.9%	21.3%	4.8%	5.6%
Audio	11.1%	53.1%	5.6%	1.6%

Table 9: Percentage of fingerprinting scripts blocked by Disconnect or the combination of EasyList and EasyPrivacy for all techniques described in Section 6. Included is the percentage of sites with fingerprinting scripts on which scripts are blocked.

Fingerprinting scripts pose a unique challenge for manually curated block lists. They may not change the rendering of a page or be included by an advertising entity. The script content may be obfuscated to the point where manual inspection is difficult and the purpose of the script unclear.

OpenWPM's active instrumentation (see Section 3.2) detects a large number of scripts not blocked by the current privacy tools. Disconnect and a combination of EasyList and EasyPrivacy both perform similarly in their block rate. The privacy tools block canvas fingerprinting on over 78% of sites, and block canvas font fingerprinting on over 90%. However, only a fraction of the total number of scripts utilizing the techniques are blocked (between 10% and 25%) showing that less popular third parties are missed. Lesser-known techniques, like WebRTC IP discovery and Audio fingerprinting have even lower rates of detection.
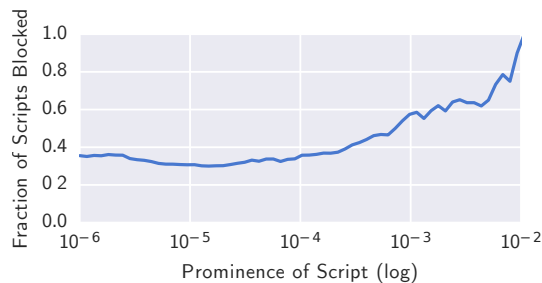
Figure 8: Fraction of fingerprinting scripts with prominence above a given level blocked by Disconnect, EasyList, or EasyPrivacy on the top 1M sites.

In fact, fingerprinting scripts with a low prominence are blocked much less frequently than those with high prominence. Figure 8 shows the fraction of scripts which are blocked by Disconnect, EasyList, or Easyprivacy for all techniques analyzed in this section. 90% of scripts with a prominence above 0.01 are detected and blocked by one of the blocking lists, while only 35% of those with a prominence above 0.0001 are. The long tail of fingerprinting scripts are largely unblocked by current privacy tools.

7. CONCLUSION AND FUTURE WORK

Web privacy measurement has the potential to play a key role in keeping online privacy incursions and power imbalances in check. To achieve this potential, measurement tools must be made available broadly rather than just within the research community. In this work, we've tried to bring this ambitious goal closer to reality. The analysis presented in this paper represents a snapshot of results from ongoing, monthly measurements. Our Platform and census measurements are the first two stages of a multi-year project. The first is the use of machine learning to automatically detect and classify trackers. The second is a web-based analysis platform that makes it easy for a minimally technically skilled analyst to investigate online tracking based on the data we make available.

8. ACKNOWLEDGEMENTS

9. REFERENCES

[1] G. Acar, C. Eubank, S. Englehardt, M. Juarez, A. Narayanan, and C. Diaz. The web never forgets: Persistent tracking mechanisms in the wild. In *Proceedings of CCS*, 2014.

[2] G. Acar, M. Juarez, N. Nikiforakis, C. Diaz, S. Gürses, F. Piessens, and B. Preneel. FPDetective: dusting the web for fingerprinters. In *Proceedings of CCS*. ACM, 2013.

[3] L. A. Adamic and B. A. Huberman. Zipf's law and the internet. *Glottometrics*, 3(1):143–150, 2002.

[4] H. C. Altaweel I, Good N. Web privacy census. *Technology Science*, 2015.

[5] J. Angwin. What they know. The Wall Street Journal. http://online.wsj.com/public/page/what-they-know-digital-privacy.html, 2012.

[6] M. Ayenson, D. J. Wambach, A. Soltani, N. Good, and C. J. Hoofnagle. Flash cookies and privacy II: Now with HTML5 and ETag respawning. *World Wide Web Internet And Web Information Systems*, 2011.

[7] P. E. Black. Ratcliff/Obershelp pattern recognition. http://xlinux.nist.gov/dads/HTML/ratcliffObershelp.html, Dec. 2004.

[8] Bugzilla. WebRTC Internal IP Address Leakage. https://bugzilla.mozilla.org/show_bug.cgi?id=959893.

[9] A. Datta, M. C. Tschantz, and A. Datta. Automated experiments on ad privacy settings. *Privacy Enhancing Technologies*, 2015.

[10] P. Eckersley. How unique is your web browser? In *Privacy Enhancing Technologies*. Springer, 2010.

[11] Electronic Frontier Foundation. Encrypting the Web. https://www.eff.org/encrypt-the-web.

[12] S. Englehardt, D. Reisman, C. Eubank, P. Zimmerman, J. Mayer, A. Narayanan, and E. W. Felten. Cookies that give you away: The surveillance implications of web tracking. In *24th International Conference on World Wide Web*, pages 289–299. International World Wide Web Conferences Steering Committee, 2015.

[13] Federal Trade Commission. Google will pay $22.5 million to settle FTC charges it misrepresented privacy assurances to users of Apple's Safari internet browser. https://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented, 2012.

[14] D. Fifield and S. Egelman. Fingerprinting web users through font metrics. In *Financial Cryptography and Data Security*, pages 107–124. Springer, 2015.

[15] N. Fruchter, H. Miao, S. Stevenson, and R. Balebako. Variations in tracking in relation to geographic location. In *Proceedings of W2SP*, 2015.

[16] C. J. Hoofnagle and N. Good. Web privacy census. *Available at SSRN 2460547*, 2012.

[17] M. Kranch and J. Bonneau. Upgrading HTTPS in midair: HSTS and key pinning in practice. In *NDSS '15: The 2015 Network and Distributed System Security Symposium*, February 2015.

[18] S. A. Krashakov, A. B. Teslyuk, and L. N. Shchur. On the universality of rank distributions of website popularity. *Computer Networks*, 50(11):1769–1780, 2006.

[19] B. Krishnamurthy and C. Wills. Privacy diffusion on the web: a longitudinal perspective. In *Conference on World Wide Web*. ACM, 2009.

[20] P. Laperdrix, W. Rudametkin, and B. Baudry. Beauty and the beast: Diverting modern web browsers to build unique browser fingerprints. In *37th IEEE Symposium on Security and Privacy (S&P 2016)*, 2016.

[21] M. Lécuyer, G. Ducoffe, F. Lan, A. Papancea, T. Petsios, R. Spahn, A. Chaintreau, and R. Geambasu. Xray: Enhancing the web's transparency with differential correlation. In *USENIX Security Symposium*, 2014.

[22] T. Libert. Exposing the invisible web: An analysis of third-party http requests on 1 million websites. *International Journal of Communication*, 9(0), 2015.

[23] J. R. Mayer and J. C. Mitchell. Third-party web tracking: Policy and technology. In *Security and Privacy (S&P)*. IEEE, 2012.

[24] A. M. McDonald and L. F. Cranor. Survey of the use of Adobe Flash Local Shared Objects to respawn HTTP cookies, a. *ISJLP*, 7, 2011.

[25] K. Mowery and H. Shacham. Pixel perfect: Fingerprinting canvas in html5. *Proceedings of W2SP*, 2012.

[26] Mozilla Developer Network. Mixed content - Security. https://developer.mozilla.org/en-US/docs/Security/Mixed_content.

[27] C. Neasbitt, B. Li, R. Perdisci, L. Lu, K. Singh, and K. Li. Webcapsule: Towards a lightweight forensic engine for web browsers. In *Proceedings of CCS*. ACM, 2015.

[28] N. Nikiforakis, L. Invernizzi, A. Kapravelos, S. Van Acker, W. Joosen, C. Kruegel, F. Piessens, and G. Vigna. You are what you include: Large-scale evaluation of remote javascript inclusions. In *Proceedings of CCS*. ACM, 2012.

[29] N. Nikiforakis, A. Kapravelos, W. Joosen, C. Kruegel, F. Piessens, and G. Vigna. Cookieless monster: Exploring the ecosystem of web-based device fingerprinting. In *Security and Privacy (S&P)*. IEEE, 2013.

[30] F. Ocariza, K. Pattabiraman, and B. Zorn. Javascript errors in the wild: An empirical study. In *Software Reliability Engineering (ISSRE)*. IEEE, 2011.

[31] L. Olejnik, G. Acar, C. Castelluccia, and C. Diaz. The leaking battery. *Cryptology ePrint Archive*, Report 2015/616, 2015.

[32] Phantom JS. Supported web standards. http://www.webcitation.org/6hI3iptm5, 2016.

[33] M. Z. Rafique, T. Van Goethem, W. Joosen, C. Huygens, and N. Nikiforakis. It's free for a reason: Exploring the ecosystem of free live streaming services. In *Network and Distributed System Security (NDSS)*, 2016.

[34] N. Robinson and J. Bonneau. Cognitive disconnect: Understanding Facebook Connect login permissions. In *2nd ACM conference on Online social networks*. ACM, 2014.

[35] F. Roesner, T. Kohno, and D. Wetherall. Detecting and Defending Against Third-Party Tracking on the Web. In *Symposium on Networking Systems Design and Implementation*. USENIX, 2012.

[36] S. Schelter and J. Kunegis. On the ubiquity of web tracking: Insights from a billion-page web crawl. *arXiv preprint arXiv:1607.07403*, 2016.

[37] Selenium Browser Automation. Selenium faq. https://code.google.com/p/selenium/wiki/FrequentlyAskedQuestions, 2014.

[38] K. Singh, A. Moshchuk, H. J. Wang, and W. Lee. On the incoherencies in web browser access control policies. In *Proceedings of S&P*. IEEE, 2010.

[39] A. Soltani, S. Canty, Q. Mayo, L. Thomas, and C. J. Hoofnagle. Flash cookies and privacy. In *AAAI Spring Symposium: Intelligent Information Privacy Management*, 2010.

[40] O. Starov, J. Dahse, S. S. Ahmad, T. Holz, and N. Nikiforakis. No honor among thieves: A large-scale analysis of malicious web shells. In *International Conference on World Wide Web*, 2016.

[41] Z. Tollman. We're Going HTTPS: Here's How WIRED Is Tackling a Huge Security Upgrade. https://www.wired.com/2016/04/wired-launching-https-security-upgrade/, 2016.

[42] J. Uberti. New proposal for IP address handling in WebRTC. https://www.ietf.org/mail-archive/web/rtcweb/current/msg14494.html.

[43] J. Uberti and G. wei Shieh. WebRTC IP Address Handling Recommendations. https://datatracker.ietf.org/doc/draft-ietf-rtcweb-ip-handling/.

[44] S. Van Acker, D. Hausknecht, W. Joosen, and A. Sabelfeld. Password meters and generators on the web: From large-scale empirical study to getting it right. In *Conference on Data and Application Security and Privacy*. ACM, 2015.

[45] S. Van Acker, N. Nikiforakis, L. Desmet, W. Joosen, and F. Piessens. Flashover: Automated discovery of cross-site scripting vulnerabilities in rich internet applications. In *Proceedings of CCS*. ACM, 2012.

[46] T. Van Goethem, F. Piessens, W. Joosen, and N. Nikiforakis. Clubbing seals: Exploring the ecosystem of third-party security seals. In *Proceedings of CCS*. ACM, 2014.

[47] W. V. Wazer. Moving the Washington Post to HTTPS. https://developer.washingtonpost.com/pb/blog/post/2015/12/10/moving-the-washington-post-to-https/, 2015.

[48] X. Xing, W. Meng, B. Lee, U. Weinsberg, A. Sheth, R. Perdisci, and W. Lee. Understanding malvertising through ad-injecting browser extensions. In *24th International Conference on World Wide Web*. International World Wide Web Conferences Steering Committee, 2015.

[49] C. Yue and H. Wang. A measurement study of insecure javascript practices on the web. *ACM Transactions on the Web (TWEB)*, 7(2):7, 2013.

[50] A. Zarras, A. Kapravelos, G. Stringhini, T. Holz, C. Kruegel, and G. Vigna. The dark alleys of madison avenue: Understanding malicious advertisements. In *Internet Measurement Conference*. ACM, 2014.

THE VERGE

GOOGLE \ POLICY \ TECH \

Democrats say Google must curb location tracking before Roe repeal

42 ᐟ

Without changes, Android's location system could become 'a tool for far-right extremists,' members of Congress say

By Corin Faife | @corintxt | May 24, 2022, 5:08pm EDT

Illustration by Alex Castro / The Verge

A group of more than 40 Democratic members of Congress has asked Google to stop collecting and retaining "unnecessary" location data out of fear that it could be used to identify and prosecute people who have obtained abortions.

The request was made in a letter sent to Google CEO Sundar Pichai on Tuesday by members of the House and Senate, led by Senator Ron Wyden (D-OR) and including well-known progressive representatives such as Ayanna Pressley, Elizabeth Warren, Bernie Sanders, and Alexandria Ocasio-Cortez.

"We believe that abortion is health care," the letter states. "We will fight tooth and nail to ensure that it remains recognized as a fundamental right, and that all people in the United States have control over their own bodies. That said, we are concerned that, in a world in which abortion could be made illegal, Google's current practice of collecting and retaining extensive records of cell phone location data will allow it to become a tool for far-right extremists looking to crack down on people seeking reproductive health care."

"GOOGLE'S CURRENT PRACTICE OF COLLECTING AND RETAINING EXTENSIVE RECORDS OF CELL PHONE LOCATION DATA WILL ALLOW IT TO BECOME A TOOL FOR FAR-RIGHT EXTREMISTS"

The letter specifically references geofence warrants, a controversial technique in which law enforcement agencies request that tech companies provide data on all mobile phones that passed through a geographically defined area in a certain time period. Geofence warrants have been criticized for their use in the investigation of protesters during Black Lives Matter demonstrations, and their use has grown dramatically in recent years: data released by Google showed a pronounced spike from 2018 to 2020.

Crucially, geofence data is only available after a court-issued warrant — but with more than 20 states preparing to outlaw abortion as soon as *Roe v. Wade* is overturned, it's increasingly plausible that such a warrant could be used to target anyone visiting an

abortion provider.

To prevent this from happening, the signatories of the letter request that Google redesign its location data collection practices so that device data is only collected at an aggregate level, rather than on an individual basis, and is not retained by the company for longer than needed. The letter also contrasts Google's location data policy with Apple's decision to minimize location data retention, stating that "Americans who can afford an iPhone have greater privacy from government surveillance of their movements than the tens of millions Americans using Android devices."

Reproductive rights advocates have been on high alert since a draft opinion was leaked on May 3rd suggesting that the Supreme Court intends to overturn *Roe v. Wade*. In particular, many have raised concerns that digital surveillance technology could be used to prosecute people who seek out abortions. On the same day that the Democratic letter was released, the New York-based Surveillance Technology Oversight Project published a report on the many ways that people seeking abortions might be tracked, citing a number of existing cases where data from internet search history or credit card transactions has been used against people who have terminated pregnancies.

In a statement, Albert Fox Cahn, executive director of the Surveillance Technology Oversight Project, welcomed the Congressional letter, saying that Google should delete its location data or be "complicit in criminalizing abortion."

"It's not enough for tech firms to say they're pro-choice, they have to stop collecting data that puts pregnant people at risk," Cahn said. "There's no way for Texas to station state police at every out-of-state abortion clinic, but with data from Google and other companies, they don't need to. If tech giants don't act soon, we'll see pregnant people seeking abortion care out of state, only to come home to an arrest warrant."

So far, Google has not made any public response to the letter; the company did not immediately respond to questions sent by *The Verge*.

Could not connect to the reCAPTCHA service. Please check your internet connection and reload to get a reCAPTCHA challenge.

THE VERGE

POLICY \ PRIVACY \

ICE uses data brokers to bypass surveillance restrictions, report finds

Authors of the American Dragnet study say the agency is increasingly unaccountable to legislators

By Corin Faife | @corintxt | May 10, 2022, 10:45am EDT

6 ,

Photo by RINGO CHIU/AFP via Getty Images

For almost as long as it has existed, Immigration and Customs Enforcement (ICE) has drawn criticism for the methods by which its agents pursue and remove undocumented migrants. But a new report published Tuesday sheds new light on the extent to which the agency has expanded its domestic surveillance apparatus over the course of its 19-year history.

The report, from a group of researchers at the Georgetown Law Center on Privacy & Technology, paints a picture of an agency that is able to access the personal information of hundreds of millions of Americans and does so largely without accountability through extensive deals with private data brokers.

According to details in *American Dragnet: Data-Driven Deportation in the 21st Century*, ICE has used a combination of public records and privately acquired information to build a surveillance system that can investigate the majority of US adults with little oversight. The agency now has access to the driver's license data of three-quarters of US adults (74 percent) and has already run facial recognition scans on the license photographs of 1 in 3 adults (32 percent). And when three out of four adults hooked up utilities like gas, water, and electricity in a new home, ICE was able to automatically update their new address.

"ICE HAS BUILT UP A SWEEPING SURVEILLANCE INFRASTRUCTURE THAT'S CAPABLE OF TRACKING ALMOST ANYONE SEEMINGLY AT ANY TIME"

"ICE consistently paints itself as an agency whose efforts are really focused or targeted, but we're not really seeing that at all," Nina Wang, a policy associate at Georgetown Law and co-author of the report, told *The Verge*. "Instead, what we're seeing is that ICE has built up a sweeping surveillance infrastructure that's capable of tracking almost anyone seemingly at any time. These initiatives were conducted in near-complete secrecy and impunity, sidestepping limitations and flying under the radar of most state officials. And ultimately, these surveillance tactics cross legal and ethical boundaries."

The report was compiled from the results of hundreds of freedom of information requests sent to state agencies across the country and a review of more than 100,000 ICE spending contracts. In combination, these documents were used to evaluate the type of information being made available to ICE and the nature of the technology being used to process it.

The results help to illuminate the full scope of ICE's surveillance capabilities for the first time, giving numbers to quantify the extent of programs that have been uncovered by prior research from organizations like the National Immigration Law Center or the ACLU.

Some of the findings add context to surveillance techniques that have already received public attention, like the use of data from utility companies in immigration enforcement — a practice that has been criticized for its potential to cut off undocumented migrants from enjoying basic services like power, water, or telephone connections.

"THE MASS COLLECTION OF DATA BY ICE AND OTHER LAW ENFORCEMENT AGENCIES POSES A TREMENDOUS RISK"

The report also highlights the extent to which ICE also obtains data directly and indirectly from government services like state motor vehicle departments. Currently, 16 states and the District of Columbia allow undocumented immigrants to apply for driver's licenses, but the Georgetown report finds that ICE can search through these records without a warrant in at least five of the 17 jurisdictions.

"The mass collection of data by ICE and other law enforcement agencies poses a tremendous risk and has a chilling effect on people accessing critical public services," said Zach Ahmad, senior policy counsel for the New York Civil Liberties Union. "Our most vulnerable won't be protected from perpetual surveillance, tracking, and the threat of arrest or deportation until we pass fundamental digital privacy protections and give people control over their data."

While lawmakers in some states have passed laws to restrict ICE's access to

information from government bodies, the immigration agency has frequently been able to skirt such legislation by contracting with third-party data brokers to obtain the same information indirectly. The report cites a particularly stark example from Oregon: shortly after the state passed a law to prevent ICE from accessing driver's license data in 2019, Oregon's Department of Motor Vehicles signed an agreement to sell data to Thomson Reuters and LexisNexis, both of which provide data services to ICE.

Civil liberties organizations have raised concerns about the danger of public-private surveillance deals for years, but recently, the role of private companies in ICE's monitoring operations has come under increasing scrutiny thanks to efforts from groups like the Latinx social justice nonprofit Mijente, which has led a push for organizations to end contracts with ICE.

The new report outlines "one piece of the massive puzzle that is ICE digital surveillance and policing," Cinthya Rodriguez, an organizer at Mijente, told *The Verge*. "We're calling on local governments to investigate and ultimately cut contracts that share our personal information with ICE leading to detention and deportations."

"WE'RE CALLING ON LOCAL GOVERNMENTS TO INVESTIGATE AND ULTIMATELY CUT CONTRACTS THAT SHARE OUR PERSONAL INFORMATION WITH ICE"

Canadian media conglomerate Thomson Reuters is one organization that has been spotlighted by Mijente's work and now in the *American Dragnet* report. Thomson Reuters formerly contracted with ICE to provide access to a huge database known as CLEAR, though the contract was allowed to expire in 2021 after the Canadian company faced pressure from activist investors.

In an email sent to *The Verge*, Dave Moran, head of communications at Thomson Reuters, confirmed that ICE no longer had access to the CLEAR database but said that the media company still maintained other contracts with the agency.

"Thomson Reuters is engaged by DHS-ICE to support the agency's investigations involving crimes such as terrorism, national security cases, narcotics smuggling, organized crime, transnational gang activity and human trafficking," Moran said. "For

example, during the Miami Super Bowl, our work with ICE assisted law enforcement officials in saving over 20 human trafficking victims."

But in a sign of how difficult it is to prevent a federal agency like ICE from accessing private data, the expired Thomson Reuters contract was quickly replaced by a deal with LexisNexis, which signed a $16.8 million contract with ICE in 2021. The details of the LexisNexis contract reportedly give ICE access to billions of public and private records, including credit history details, license plate images, and cellular phone subscriber information.

A request for comment sent through LexisNexis' media contact form had not received a response by time of publication.

Privacy advocates hope the report will spark renewed discussion of the appropriate scope of ICE's role in American life. "ICE continues to harvest data on millions of Americans from data brokers. It's long past time for lawmakers to make clear that ICE and police can't buy their way around the Fourth Amendment," said Albert Fox Cahn, founder and executive director of the Surveillance Technology Oversight Project. "You shouldn't be able to use tax dollars to buy our Constitutional rights. And no one should fear that they'll face deportation simply for signing up for home electricity or buying a cellphone."

Phone calls made to the ICE Office of Public Affairs went unanswered. The agency had not responded to email questions sent by *The Verge* at time of publication.

Your phone could reveal if you've had an abortion

Geoffrey A. Fowler, Tatum Hunter

When someone gets an abortion, they may decide not to share information with friends and family members. But chances are their smartphone knows.

The leak of a Supreme Court draft opinion proposing to overturn *Roe v. Wade* raises a data privacy flash point: If abortion becomes criminal in some states, might a person's data trail be treated as evidence?

There is precedent for it, and privacy advocates say data collection could become a major liability for people seeking abortions in secret. Phones can record communications, search histories, body health data and other information. Just Tuesday, there was new evidence that commercial data brokers sell location information gathered from the phones of people who visit abortion clinics.

"It is absolutely something to be concerned about — and something to learn about, hopefully before being in a crisis mode, where learning on the fly might be more difficult," said Cynthia Conti-Cook, a technology fellow at the Ford Foundation.

It is now common for law enforcement to make use of the contents of people's phones, including location and browsing information. One case against an alleged Jan. 6 insurrectionist drew upon thousands of pages of data from the suspect's phone as well as Facebook records, prosecutors said.

A major data source is our digital surveillance economy — Facebook, Google and apps galore — in which companies track consumers to figure out how to sell to them. The data may change hands several times or seep into a broader marketplace run by data brokers. Such brokers can amass huge collections of information.

That data is an easy target for subpoenas, or court orders, and many tech companies do not give straight answers about what information they would be willing to hand over. Google, for one, reports that it received more than 40,000 subpoenas and search warrants in the United States in the first half of 2021.

> A leaked draft opinion on May 2 shows that the Supreme Court is poised to overturn federal abortion protections. Here's what would happen. (Video: Joshua Carroll/The Washington Post)

Police and private citizens alike could buy data and use it to investigate suspected abortions. Phone location information has been used by activist groups to target ads at people in abortion clinics to try to dissuade them.

Crunching all that data isn't easy, and law enforcement agencies have plenty of "lower-hanging fruit" to pursue, says Alan Butler, the executive director and president of the

Electronic Privacy Information Center. Those more traditional methods include checking credit card records, collecting data from cellphone towers, and talking to friends and family members.

But it is tough to predict how restrictive state abortions laws would become if *Roe v. Wade* were overturned. "Even a search for information about a clinic could become illegal under some state laws, or an effort to travel to a clinic with an intent to obtain an abortion," Butler said.

No matter what happens, the possibility of mass data-collection to enforce abortion bans will hang over the heads of people seeking abortions or helping others get them, said Nikolas Guggenberger, the executive director at the Yale Information Society Project. "People want to be on the safe side, so even if the law doesn't apply to what they're doing, it has a chilling effect," he said.

A number of groups have published citizen guides to avoiding surveillance while seeking an abortion or reproductive health care. Those groups include the Digital Defense Fund, the Repro Legal Helpline and the Electronic Frontier Foundation.

Here are three potential contributors to the data trail on people seeking abortions — and how they might be used.

Location

Phones can collect precise information about your whereabouts — right down to the building — to power maps and other services. Sometimes, though, the fine print in app privacy policies gives companies the right to sell that information to other companies that can make it available to advertisers, or whoever wants to pay to obtain it.

On Tuesday, Vice's Motherboard blog reported that for $160, it bought a week's worth of data from a company called SafeGraph showing where people who visited more than 600 Planned Parenthood clinics came from and where they went afterward.

This kind of data could be used, for example, to identify clinics that provide abortions to people from out of state in places where that is illegal.

SafeGraph CEO Auren Hoffman told The Washington Post on Tuesday that his company was discussing whether to stop offering aggregated data on physical traffic to abortion providers. SafeGraph and companies like it do not usually sell the location information linked to names or phone numbers, although the company has come under fire from privacy advocates before and has changed some of its practices to make it harder to tie data to specific people.

"You can find someone to say they can de-anonymize the data, but if it could be done, someone would have written a paper by now," Hoffman said.

But privacy watchdogs say you can learn a lot by connecting the dots on multiple places a single person has visited. For example, last year, a Catholic blog obtained location information originally generated by the dating app Grindr to out a priest as gay. Those behind the blog were able to infer that a person at a church-related location also was visiting gay bars.

Apple and Android phones offer settings to turn off location services for individual apps — or entirely for the phone. But doing so might prevent the operation of certain functions, such as transportation apps.

Search and chat histories

Searching for information about clinics and medications can leave a trail of records with Google, which in some cases saves queries to a user's profile.

In 2017, prosecutors used Internet searches for abortion drugs as evidence in a Mississippi woman's trial for the death of her fetus. A grand jury ultimately decided not to pursue charges, according to National Advocates for Pregnant Women. And last year, the Supreme Court of Wisconsin decided that detectives did not violate the rights of the convicted murderer George Burch when, operating without a warrant, they accessed downloaded data from his phone, including his Internet search history.

Private messages also can become evidence. In 2015, text messages about getting an abortion helped convict a woman of child neglect and feticide.

A 2020 report by Upturn, a nonprofit organization focused on technology and justice, found that law enforcement agencies use "mobile device forensic tools" — which can give them access to Internet histories as well as to unencrypted emails and texts — when investigating matters as varied as marijuana possession and graffiti.

People can take some steps to keep their search and chat histories private. Ford Foundation's Conti-Cook said people do not have to volunteer their phones when police ask, and they can opt for encrypted messaging apps and a virtual private network, or VPN, to obscure their identities while conducting searches.

Reproductive health apps

Millions of people use apps to help track their menstrual cycles, logging and storing intimate data about their reproductive health. Because that data can reveal when periods, ovulation and pregnancy stops and starts, it could become evidence in states where abortion is criminalized.

There is evidence that these companies play fast and loose with privacy. In 2019, the period tracker Ovia got pushback for sharing aggregate data on some users' family planning with their employers.

Last year, the Federal Trade Commission settled with the period-tracking app Flo after the app promised to keep users' data private but then shared it with marketing firms including Facebook and Google.

A recent investigation by Consumer Reports found shortcomings in the way five popular period-tracking apps handle the sensitive user data, including sending it to third parties for targeted advertising.

How are the apps allowed to share such personal data? Our interactions with health-care providers are covered by a federal privacy law called the Health Insurance Portability and Accountability Act, or HIPAA. However, period-tracking apps aren't defined as covered entities, so they can legally share data.

Joseph Menn contributed to this report.

About the Cross Device reports

Connect data from multiple sessions to see the conversion process from start to finish.

The Cross Device reports give you the tools you need to organize data across multiple devices into a cohesive analysis, so you get a better idea of how seemingly unrelated touch points, sessions, and interactions are connected.

For example, you might discover that one segment of users searches on a mobile device and purchases on a tablet within the same day, while another segment clicks an ad on a mobile device, browses your site on a desktop the next day, and returns to make a purchase on a tablet a week later.

The Cross Device reports help you connect data about devices and activities from different sessions so you can get a better understanding of your users and what they do at each step of the conversion process - from initial contact to long-term retention.

Access the Cross Device reports

The Cross Device reports are only available in User ID views. You must first set up the User ID and create a User ID view in your account before you can access these reports.

Related resources

You can find the Cross Device reports in the *Audience* section of a reporting view. Learn about each of the Cross Device reports:

- Device Overlap: Find out what type and how many devices are used to access your content.
- Device Paths: Discover the last 5 device types used before a conversion.
- Acquisition Device: See the relationship between acquisitions and conversions.

About the User-ID feature

Connect multiple devices, sessions, and engagement data to the same users.

User-ID lets you associate a persistent ID for a single user with that user's engagement data from one or more sessions initiated from one or more devices.

Analytics interprets each unique user ID as a separate user, which provides a more accurate user count in your reports.

When you send Analytics an ID and related data from multiple sessions, your reports tell a more unified, holistic story about a user's relationship with your business.

In this article:

[How User-ID works](#)
[Session Unification](#)
[Next steps](#)
[Related resources](#)

How User-ID works

User-ID enables the association of one or more sessions (and the activity within those sessions) with a unique and persistent ID that you send to Analytics.

To implement User-ID, you must be able to generate your own unique IDs, consistently assign IDs to users, and include these IDs wherever you send data to Analytics.

For example, you could send the unique IDs generated by your own authentication system to Analytics as values for User-ID. Any engagement, like link clicks and page or screen navigation, that happen while a unique ID is assigned can be sent to Analytics and connected via User-ID.

In an Analytics implementation without the User-ID feature, a unique user is counted each time your content is accessed from a different device and each time there's a new session. For example, a search on a phone one day, purchase on a laptop three days later, and request for customer service on a tablet a month after that are counted as three unique users in a standard Analytics implementation, even if all those actions took place while a user was signed in to an account. While you can collect data about each of those interactions and devices, you can't determine their relevance to one another. You only see independent data points.

When you implement User-ID, you can identify related actions and devices and connect these seemingly independent data points. That same search on a phone, purchase on a laptop, and re-engagement on a tablet that previously looked like three unrelated actions on unrelated devices can now be understood as one user's interactions with your business.

Session unification

Session unification is a User-ID setting that allows hits collected before a user ID is assigned to be associated with the ID.

[Learn more](#)

Next steps

To set up User-ID, you must first enable the feature in your Analytics account ([Editor role](#) required), and then modify your tracking code. [Learn more](#)

You can verify your setup by checking the data in the [User-ID Coverage report](#).

Related resources

Refer to the Developer documentation for information on how to add the User-ID to your tracking code.

- **Websites:** [gtag.js](#)

Case 4:20-cv-03664-YGR   Document 928-20   Filed 04/19/23   Page 114 of 405

- **Mobile apps:** Android apps   or iOS apps

Google Analytics opt-out browser add-on

You can opt-out of having your site activity available to Google Analytics by installing the Google Analytics opt-out browser add-on . The add-on prevents the Google Analytics JavaScript (gtag.js, analytics.js) that is running on websites from sharing information with Google Analytics about visit activity.

Using the Google Analytics opt-out browser add-on will not prevent site owners from using other tools to measure site analytics. It does not prevent data from being sent to the website itself or in other ways to web analytics services.

User-ID and Cross Device

User-ID is a Universal Analytics feature that you can use to associate multiple sessions (and any activity within those sessions) with a unique ID. With it, you can get a more accurate user count, analyze the signed-in user experience, and get access to the Cross Device reports. Learn more about Universal Analytics

The Cross Device reports give you the tools you need to organize data across multiple devices into a cohesive analysis, so you get a better idea of how different devices, sessions, and interactions are connected to each other.

User-ID feature set up

About the User-ID feature

Benefits of User-ID

Set up User-ID

User-ID limits

User-ID Coverage report

Session unification

User-ID reference

User-ID views and Cross Device reports

About User-ID views

Limits of User-ID views & Cross Device reports

About the Cross Device reports

Case 4:20-cv-03664-YGR   Document 928-20   Filed 04/19/23   Page 117 of 405

Device Overlap

Device Paths

Acquisition Device

Policy requirements for Google Analytics Advertising Features

This article applies to both Google Analytics 4 and Universal Analytics.

Google Analytics Advertising Features let you enable features in Analytics that aren't available through standard implementations. Advertising features include:

- Remarketing with Google Analytics

- Google Display Network Impression Reporting

- Google Analytics Demographics and Interest Reporting

- Integrated services that require Google Analytics to collect data for advertising purposes, including the collection of data via advertising cookies and identifiers

By enabling the Advertising Features, you enable Google Analytics to collect data about your traffic via Google advertising cookies and identifiers, in addition to data collected through a standard Google Analytics implementation. Regardless of how you send data to Google Analytics (for example, via the Google Analytics tracking code, Google Analytics SDK, or the Measurement Protocol), if you use Google Analytics Advertising Features, you must adhere to this policy.

When you use Google Analytics Advertising Features, you are the sole controller under all applicable data protection legislation.

This means you will not identify users or facilitate the merging of personally identifiable information with additional information collected through any Google advertising product or feature unless you have robust notice of, and the user's prior affirmative (i.e., opt-in) consent to, that identification or merger, and are using a Google Analytics feature that expressly supports such identification or merger. Irrespective of users' consent, you must not attempt to disaggregate data that Google reports in aggregate.

Learn more about PII in Google's contracts and policies

If you've enabled any Google Analytics Advertising features, you are required to notify your visitors by disclosing the following information in your privacy policy:

- The Google Analytics Advertising Features you've implemented.

- How you and third-party vendors use first-party cookies (such as the Google Analytics cookie) or other first-party identifiers, and third-party cookies (such as Google advertising cookies) or other third-party identifiers together.

- How visitors can opt-out of the Google Analytics Advertising Features you use, including through Ads Settings, Ad Settings for mobile apps, or any other available means (for example, the NAI's consumer opt-out).

We also encourage you to point users to Google Analytics' currently available opt-outs for the web.

European Union user-consent policy

When using Google Analytics Advertising Features, you must also comply with the European Union User Consent Policy.

Japan user-consent policy

If you receive non-personally identifiable user information relating to Japanese users from Google in connection with your use of Google Analytics, you must not merge that information with personally-identifiable information unless, prior to such processing, you have obtained all legally required consents from the user and have provided Google with accurate and complete information about the processing via the Google Troubleshooter.

Interest-based advertising

If you've enabled interest-based advertising, including Remarketing, with Google Analytics in connection with other Google services, you must follow the policies applicable to those Google services (like the Google Ads Policy for Personalized advertising and its sensitive category restrictions, and the Platform Program Policies). If you

use Google Analytics to collect sensitive information about your visitors, as described in the Google Ads sensitive category restrictions, you may not use Google Analytics to collect data for the purpose of interest based advertising. You can disable interest-based advertising via the advanced ads-personalization setting.

Because laws across countries and territories vary, and because Google Analytics can be used in many ways, Google is unable to provide the exact language you need to include in your privacy policy. Only you understand the unique aspects and special considerations of your business, and your privacy policy should account for this information that only you can provide.

This policy was last updated April 27, 2022.

Browse in private

If you don't want Google Chrome to remember your activity, you can browse the web privately in Incognito mode.

Computer   Android   iPhone & iPad

1. On your computer, open Chrome.
2. At the top right, click More ⋮ ＞ **New Incognito Window**.
3. A new window appears. In the top corner, check for the Incognito icon 🕵️ .

You can also use a keyboard shortcut to open an Incognito window:

- Windows, Linux, or Chrome OS: Press **Ctrl + Shift + n**.
- Mac: Press **⌘ + Shift + n**.

You can switch between Incognito windows and regular Chrome windows. You'll only browse in private when you're using an Incognito window.

You can also choose to block third-party cookies when you open a new incognito window. Learn more about cookies.

Close Incognito mode to stop private browsing

Incognito mode runs in a separate window from your normal Chrome windows.

If you have an Incognito window open and you open another one, your private browsing session will continue in the new window. To exit Incognito mode, close all Incognito windows.

If you see a number next to the Incognito icon at the top right, you have more than one Incognito window open. To close an Incognito window:

1. On your computer, go to your Incognito window.
2. Close the window:
   - **Windows or Chrome OS:** At the top right, click Close ✕ .
   - **Mac:** At the top left, click Close ✕ .

What happens when you browse privately

- Chrome won't save your browsing history, cookies and site data, or information entered in forms.
- Files you download and bookmarks you create will be kept.
- Your activity isn't hidden from websites you visit, your employer or school, or your internet service provider.

Learn more about how private browsing works.

Related articles

- How private browsing works
- Let others browse Chrome as a guest
- Clear Chrome browsing data

How Chrome Incognito keeps your browsing private

Incognito mode can help keep your browsing private from other people who use your device.

How Incognito mode works

When you first open a new Incognito window, you're creating a new Incognito browsing session. Any Incognito windows you open after that are part of the same session. You can end that Incognito session by closing all open Incognito windows.

In Incognito, none of your browsing history, cookies and site data, or information entered in forms are saved on your device. This means your activity doesn't show up in your Chrome browser history, so people who also use your device won't see your activity. Websites see you as a new user and won't know who you are, as long as you don't sign in.

If you're browsing in Chrome Incognito mode, you are, by default, not signed into any accounts or sites.

Your school, Internet Service Provider, or any parental tracking software may be able to see your activity. You can check if your Chrome browser is managed.

You can choose to block third-party cookies when you open a new incognito window. Learn more about cookies.

How Incognito mode protects your privacy

What Incognito mode does

- Browsing in Incognito mode means your activity data isn't saved on your device, or to a Google Account you're not signed into.
  - For example, you may use Incognito mode to shop online for a birthday gift for a family member who shares your device. If you don't sign in to your Google account, your shopping activity will not appear in your Chrome browsing activity and won't be saved to your Google Account.
- Each time you close all Incognito windows, Chrome discards any site data and cookies associated with that browsing session.
- Chrome doesn't tell websites, including Google, when you're browsing privately in Incognito mode.

What Incognito mode doesn't do

- Prevent you from telling a website who you are. If you sign in to any website in Incognito mode, that site will know that you're the one browsing and can keep track of your activities from that moment on.
- Prevent your activity or location from being visible to the websites you visit, your school, employer, or your Internet Service provider.
- Prevent the websites you visit from serving ads based on your activity during an Incognito session. After you close all Incognito windows, websites won't be able to serve ads to you based on your signed-out activity during that closed session.

You're in control

- Close all Incognito windows and tabs when you're done browsing. You end a session when you close all Incognito windows, so closing a single tab won't discard your data. If you see a number next to the Incognito icon on your desktop or at the bottom of your browser on a mobile device, you have more than one Incognito window or tab open.
- You can choose to sign in to any account when in Incognito mode. If you sign into a Google service, like Gmail, or a site, that site may remember your activity.
- Delete any downloads and bookmarks you don't want your device to remember. Files you download and bookmarks you create are saved in any mode.

Learn more about using Incognito mode.

Case 4:20-cv-03664-YGR   Document 928-20   Filed 04/19/23   Page 122 of 405

How private browsing works in Chrome

When you browse privately, other people who use the device won't see your history.

Chrome doesn't save your browsing history or information entered in forms. Cookies and site data are remembered while you're browsing, but deleted when you exit Incognito mode. You can choose to block third-party cookies when you open a new incognito window. Learn more about cookies.

What happens when you browse privately

Some information will not be seen or saved

Once you exit all your Incognito browsing windows, Chrome won't save:

- Your browsing history
- Your cookies and site data
- Information you entered in forms
- Permissions you give websites

To exit Incognito mode, close all Incognito windows.

Your activity might still be visible

Incognito mode stops Chrome from saving your browsing activity to your local history. Your activity, like your location, might still be visible to:

- Websites you visit, including the ads and resources used on those sites
- Websites you sign in to
- Your employer, school, or whoever runs the network you're using
- Your internet service provider
- Search engines
  - Search engines may show search suggestions based on your location or activity in your current Incognito browsing session. When you search on Google, Google will always estimate the general area that you're searching from. Learn more about location when you search on Google.

Some of your info might still be visible

A web service, website, search engine, or provider may be able to see:

- Your IP address, which can be used to identify the general area you're in
- Your activity when you use a web service
- Your identity if you sign in to a web service, like Gmail

You can still find and use your payment, password and contact info, but you can't change your saved info in a Chrome Incognito window.

Downloads and bookmarks are saved

Chrome won't store the files you download while browsing in private. But, they're still saved to your Downloads folder, even after you exit Incognito. You and anyone who uses your device can see and open the files.

All bookmarks you create are saved to Chrome.

Some of your preferences, including accessibility choices and bookmark settings, may also be saved to Chrome.

Computer   Android   iPhone & iPad

You can switch between Incognito windows and regular Chrome windows. You'll only browse in private when you're using an Incognito window.

You can also choose to block third-party cookies when you open a new incognito window. Learn more about cookies.

Close Incognito mode to stop private browsing

Incognito mode runs in a separate window from your normal Chrome windows.

If you have an Incognito window open and you open another one, your private browsing session will continue in the new window. To exit Incognito mode, close all Incognito windows.

If you see a number next to the Incognito icon at the top right, you have more than one Incognito window open. To close an Incognito window:

1. On your computer, go to your Incognito window.
2. Close the window:
   - **Windows or Chrome OS:** At the top right, click Close ✕.
   - **Mac:** At the top left, click Close ✕ .

Related articles

- Browse in private
- Let others browse Chrome as a guest
- Clear Chrome browsing data

Search results for "analytics opt out"

🗩 **Slow internet speeds with Chrome - Google ...**

Community forum - Google Chrome

4/10/2019 - Internet speed tests are 70% slower when using Chrome. I'm using speedtest.net. I have cleared everything, turned off extensions, and other recommended ...

👍 1023 Upvotes   🗩 79 Replies

Use Google Maps in Incognito mode

You now have more ways to control your privacy on Google Maps. Use Incognito mode when you don't want your activity—like the places you search for or navigate to—to be saved to your Google Account.

Important: When Incognito mode is on, Maps on that device will not:

- Save your browsing or search history in your account, or send notifications.
- Update your Location History or shared location, if any.
- Use your activity to personalize Maps.

Turning on Incognito mode in Maps does not affect how your activity is used or saved by internet providers, other apps, voice search, and other Google services.

Android   iPhone & iPad

Turn on Incognito mode for Google Maps

1. On your Android phone or tablet, open the Google Maps app 📍 .
2. In the top right, tap your profile picture.
3. Tap **Turn on Incognito mode**.

Turn off Incognito mode for Google Maps

1. On your Android phone or tablet, open the Google Maps app 📍 .
2. In the top right, tap your profile picture.
3. Tap **Turn off Incognito mode**.

Here are some features that aren't available in Incognito mode:

- Commute
- Following
- Location History
  - **Tip:** Location History will be paused for your entire device, not just Maps.
- Location Sharing
- Notifications and messages
- Search history
- Search completion suggestions
- Google Maps Contributions
- Google Assistant microphone in Navigation
- Offline Maps
- Your Places
- Media integration

Tip: During Maps incognito mode, the Google Assistant microphone isn't available in navigation, but "Ok Google" will continue to work as expected. Google Assistant is a system feature that isn't a part of Incognito mode for Maps, so any information you share with it will be saved as usual.

Google

"analytics opt out" site:https://support.google.com/chrome

Sign in

All   News   Images   Videos   Shopping   More   Tools

1 result (0.22 seconds)

https://support.google.com › chrome › thread › slow-inter...

Slow internet speeds with Chrome - Google Support
Apr 10, 2019 — Seems like every extension slows it down a little bit. But I found out his one
extension cuts it in 1/2. Culprit: Google **Analytics** **Opt-out** Add- ...

New York - Based on your past ac ivity - Update loca ion

Help   Send feedback   Privacy   Terms

Select a language ⌄

Google Analytics Opt-out Browser Add-on

To provide website visitors the ability to prevent their data from being used by Google Analytics, we have developed the Google Analytics opt-out browser add-on for websites using the supported version of Google Analytics JavaScript (analytics.js, gtag.js).

If you want to opt-out, download and install the add-on for your web browser. The Google Analytics opt-out add-on is designed to be compatible with Chrome, Safari, Firefox and Microsoft Edge. In order to function, the opt-out add-on must be able to load and execute properly on your browser. Learn more about about the opt-out and how to properly install the browser add-on here.

Get Google Analytics Opt-out Browser Add-on

Available for Google Chrome, Mozilla Firefox, Apple Safari and Microsoft Edge.

Learn more about Google Analytics Privacy »

Computer scientist identifies JavaScript vulnerability in thousands of websites

Catherine Graham

ProbeTheProto framework developed by computer scientist Yinzhi Cao helps identify and alert websites vulnerable to a flaw that allows malicious actors to 'pollute' important web code

Millions of developers use JavaScript to build websites and mobile apps, making it one of the most popular programming languages in the world. But according to Johns Hopkins researchers, thousands of JavaScript websites are vulnerable to a security flaw that could result in manipulating the site's URL or stealing a user's profile information.

Known as prototype pollution, the flaw allows attackers to modify, or "pollute," a prototype, which is a built-in property of a JavaScript object. An attacker who manages to alter a JavaScript object prototype can execute a variety of malicious actions.

With a framework they call ProbeTheProto, researchers from the Johns Hopkins Information Security Institute analyzed one million websites running on JavaScript and found that more than 2,700 websites—some of them the most visited in the world—had multiple flaws that could expose them to prototype pollution.

Ten of the sites were among the top 1,000 most visited websites of the year, including Weebly.com, CNET.com, and McKinsey.com.

"Our ProbeTheProto tool can automatically and accurately detect a wide range of potential attacks. And we've found that many developers are happy that we are helping them stay ahead of cybersecurity threats."

Yinzhi Cao

Assistant professor of computer science

"Only recently have researchers started looking closely at prototype pollution and realizing it's a matter of great concern," said cybersecurity expert Yinzhi Cao, an assistant professor of computer science in the Johns Hopkins Whiting School of Engineering. "Many in the developer community may not be aware that prototype pollution vulnerabilities can have severe consequences."

In Javascript, an object is a collection of related data or functionality; for example, a user account object may contain such data as usernames, passwords, and e-mail

addresses. Once an attacker makes a change to an object prototype, it will affect how the object works throughout the entire application and opens the door for more serious vulnerabilities, Cao adds.

He and his team set out to the study this snowball effect using dynamic taint analysis, a method in which inputs to the application are labeled with a special "tainted" marker and the researchers observe how the tainted data propagates through the program. If the marker is still there at the program's output, the researchers know that the application is vulnerable to exploitable input attacks that could lead to some unplanned action.

"Imagine a very long pipe in a big black box and I want to know whether Points A and B are connected. If they are, I can put some toxic liquid at Point A to attack Point B. What we do is to drop a bit of red dye in the water at Point A and then observe the water color at Point B. If I can see Point B is also red, I know A and B are connected and then we can launch attacks," Cao said.

The researchers identified three major input attacks that can be caused by prototype pollution: cross-site scripting (XSS), cookie manipulation, and URL manipulation. Such vulnerabilities on public websites provide ample opportunities for cyber criminals to hijack passwords and install malware, among other nefarious activities.

Cao says that researchers have a responsibility to report prototype pollution vulnerabilities to website owners and even recommend the best patch for their code. Thanks to Cao's team sounding the alarm, so far 293 vulnerabilities have already been fixed by developers.

"Organizations don't even know these vulnerabilities exist. Our ProbeTheProto tool can automatically and accurately detect a wide range of potential attacks. And we've found that many developers are happy that we are helping them stay ahead of cybersecurity threats," Cao said.

Computer science graduate students Zifeng Kang and Song Li contributed to the research. The team members will present their paper "Probe the Proto: Measuring Client-Side Prototype Pollution Vulnerabilities of One Million Real-world Websites," at the Network & Distributed System Security Symposium April 24-28 in San Diego.

Google Analytics To Stop Logging IP Addresses And Sunset Old Versions In Privacy Standards Overhaul

James Hercher

Updating The Platform

Major changes are coming to Google Analytics as the company navigates higher consumer privacy standards and increasingly complex international privacy laws.

For one, Universal Analytics (UA), the web-based legacy analytics product, is on the way out, and will be shuttered entirely by July 2023, the company announced on Wednesday.

All analytics customers will transition to Google Analytics 4 (GA4), which accommodates both web and app data collection and comes with built-in privacy features, not to mention a bevy of integrations across the Google portfolio, with metrics and features tied to YouTube, Search and the Google Cloud Platform.

Getting rid of UA is akin to Google's decision last year to ditch last-click attribution in favor of data-driven attribution – which relies on modeled conversions, not deterministic user-level conversions – as its default metric. Which is to say, it's about time Google cleared out the cobwebs of legacy digital advertising products.

But some of today's news is surprising and will mean major changes for some digital media and advertisers.

The most consequential change: Google Analytics will no longer log or store IP address information.

Unlike previous versions of Google Analytics, GA4 only ever used anonymized IP addresses.

"Now, we're going even further and removing IP addresses altogether," Google Analytics product director Russ Ketchum tells AdExchanger in an email.

GA4 was built post-GDPR for a digital media landscape with much higher privacy standards. Part of that re-engineering for privacy requires removing the IP address as a mechanism for tracking and analytics.

Though Ketchum also said the company isn't logging IPs "because we don't need to anymore."

Filling the IP address hole

What replaces such a strong signal for location and identity? Google has incorporated more modeled data into its analytics, such as data-driven attribution, which is natively integrated into GA4. Google also infers the approximate location data because it registers the country or market where a user is browsing.

So there are some signals, even without the individual's IP address. GA4 customers still need to tell whether a web or app visitor is in one country or another – which could be important when there are different standards for data collection or ad targeting.

Losing legal battle for the IP address

Aside from the user privacy angle, Google Analytics is under fire in EU countries because the Schrems II ruling from last year prohibits Europeans' data from being shared to US servers – not for consumer privacy issues, but because of NSA surveillance practices.

Google may hope that localizing IP address visibility and preventing the data from leaving a country will relieve the pressure on Google Analytics in the EU – many EU nation regulators have outright banned its use. The Schrems II law doesn't focus on IP addresses, but IPs are the specific pieces of personal information that EU citizens (namely, Max Schrems) have used to bring suits against Google Analytics in every EU country.

GA4 will also have new country-level controls, so data collection can be fine-tuned by market or jurisdiction of a law.

Ketchum said that with data-driven attribution modeling built in and other GA4 upgrades, the loss of IP addresses "won't impact the quality of customers' reports."

IP address expiration date

Google is leaving more than a year for brands to transition from UA to GA4 so advertisers can evaluate the data sets simultaneously, Ketchum said.

"We learned from these past migrations that customers are most successful when they have long periods of overlapping data," he wrote AdExchanger.

The majority of GA4 customers have been in a "dual setup" state for more than a year, he said. Even the laggards will have plenty of time to get comfortable with the new analytics reports.

"That way, they can gain confidence in the new data, develop a comfort level with

how it compares to the past, better understand the intentional differences, and can start relying on the new version when it makes sense," he said.

And GA4 is sweetening the pill with some additional benefits.

And by "benefits," I mean Google integrations.

There's the native data-driven attribution integration, of course. GA4 also integrates directly with BigQuery, the Google cloud data warehouse product, which is new to GA4.

One metric exclusive to GA4 is YouTube Engaged Views. With UA and previous analytics versions, YouTube measurement was limited to page views and session data, when someone starts and stops a video, say, or when multiple videos are viewed one after another.

"In Google Analytics 4 these are just two of the dozens of events that can be automatically collected," Ketchum said, including purchases, user scrolling, button clicks, external links, forms submissions and video plays, as well as metrics created by the customer.

Those metrics and integrations were formerly only available to high-paying enterprise customers. Now they're embedded in analytics for all advertisers.

And since GA4 is inherently web-and-app, whereas UA was all about the web, it also comes with integrations with the Google app developer toolkit Firebase, the Google Play Store and AdMob, Google's in-app advertising network.

Welcome to the new Google, featuring Google.

Privacy Policy

Last Updated 8/24/22

This page informs you of our policies regarding the collection, use and disclosure of Personal Information we receive from users of the Site.

We use your Personal Information only for providing and improving the Site. By using the Site, you agree to the collection and use of information in accordance with this policy.

Information Collection And Use

While using our Site, we may ask you to provide us with certain personally identifiable information that can be used to contact or identify you. Personally identifiable information may include, but is not limited to your name ("Personal Information").

Log Data

Like many site operators, we collect information that your browser sends whenever you visit our Site ("Log Data").

This Log Data may include information such as your computer's Internet Protocol ("IP") address, browser type, browser version, the pages of our Site that you visit, the time and date of your visit, the time spent on those pages and other statistics.

In addition, we may use third party services such as G ███████ and analyze this.

The Log Data section is for businesses that use a ████ apps, like Google Analytics.

Communications

Highlands Learning Center

Let me know if you have any questions!
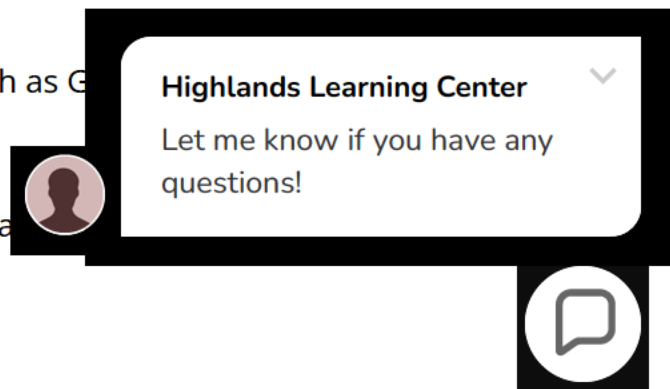
We may use your Personal Information to contact you with newsletters, marketing or promotional materials and other information that .
The Communications section is for businesses that may contact users via email (email newsletters) or other methods.

Cookies

Cookies are files with small amount of data, which may include an anonymous unique identifier. Cookies are sent to your browser from a web site and stored on your computer's hard drive.

Like many sites, we use "cookies" to collect information. You can instruct your browser to refuse all cookies or to indicate when a cookie is being sent. However, if you do not accept cookies, you may not be able to use some portions of our Site.

Security

The security of your Personal Information is important to us, but remember that no method of transmission over the Internet, or method of electronic storage, is 100% secure. While we strive to use commercially acceptable means to protect your Personal Information, we cannot guarantee its absolute security.

Changes To This Privacy Policy

This Privacy Policy is effective as of 8/24/20 and will remain in effect except with respect to any changes in its provisions in the future, which will be in effect immediately after being posted on this page.

We reserve the right to update or change our Privacy Policy at any time and you should check this Privacy Policy periodically. Your continued use of the Service after we post any modifications to the Privacy Policy on this page will constitute your acknowledgment of the modifications and your consent to abide and be bound by the modified Privacy Policy. If we make any material changes to this Privacy Policy, we will notify you either through the email address you have provided us, or by placing a prominent notice on our website.

Contact Us

If you have any questions about this Privacy Policy, please contact us.

If you wish to Opt Out click on the link here to install Google Analytics Opt-Out Add on.

Case 4:20-cv-03664-YGR   Document 928-20   Filed 04/19/23   Page 136 of 405

Home

Admissions

Contact Us

Privacy Policy

Highland Community Learning Center

5120 Godown Road, Columbus, Ohio 43220, United States

614-210-0830

‹ ▪ 4 ›

Most Common Security Vulnerabilities Using JavaScript

August 24th, 2020 by Michael Hollander
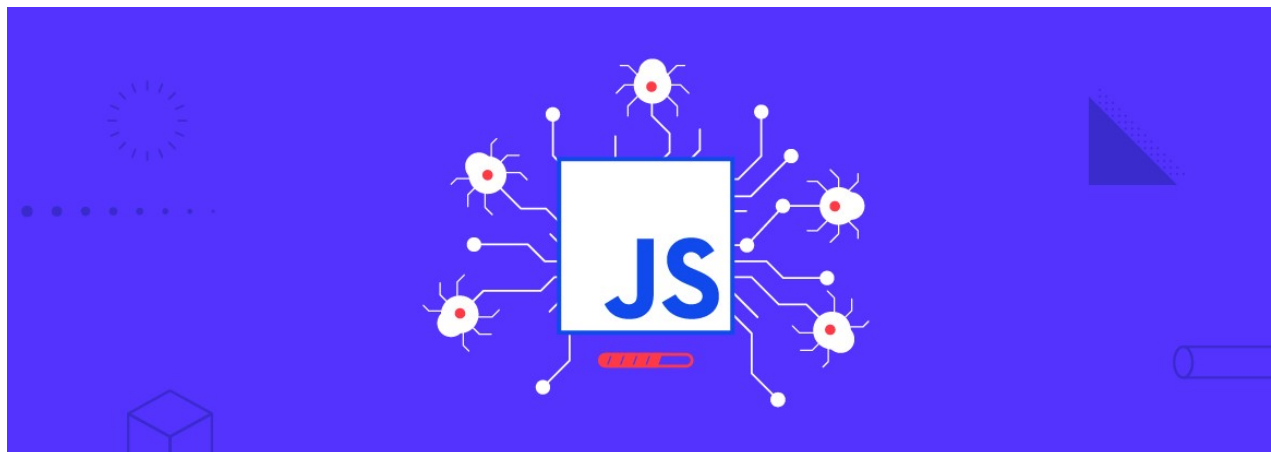
JavaScript is undoubtedly the most popular programming language for web development. A survey by Stack Overflow shows that over 67% of professional developers use JavaScript. Additionally, it is used by more than 95% of websites on the web.

From a security perspective, JavaScript is fourth on the list of the most vulnerable languages – only behind Java, PHP, and C. For this reason, developers must remain proactive and defensive in securing their JavaScript applications to keep the web safe.

This post dives into common JavaScript vulnerabilities, the risks they pose, and how developers can address these vulnerabilities to keep their web applications secure.

Cross-Site Scripting

According to OWASP, cross-site scripting (XSS) is one of the most widespread security risks in web applications. It occurs when an attacker injects malicious code into the client-side of an application. This normally happens when an application accepts untrusted (or user-supplied) data on a web page without escaping or validating it properly.

A successful XSS attack occurs when the browser executes the malicious scripts from in a manner determined by the threat actor. Generally, XSS attacks will require some form of interaction from the victim, either through social engineering or request to visit a particular page.

If an attacker exploits XSS vulnerabilities, they could perform malicious actions like account tampering, data theft, remote control, or even malware distribution.

To prevent XSS attacks, developers should separate untrusted data or user input from the active browser content. In JavaScript, you can achieve this by:

- Validating and sanitizing input from users to ensure it only contains acceptable characters that cannot be used to launch XSS attacks.

- Using safe methods such as innerText for manipulating the DOM. Unlike innerHTML, this method escapes dangerous content, thereby preventing DOM-based XSS.

- Using frameworks that automatically escape XSS vulnerabilities by design. For instance, Node JS has the encodeURI and encodeURIComponent global functions that help prevent XSS attacks. You should also consider using advanced packages like the xss-filters .

The following code snippet shows how to use XSS filters from the npm package in express applications.

```javascript
const express = require('express');
const xssFilters = require('xss-filters');
const util = require('util');
const app = express();
app.get('/', (req, res) => {    const unsafeFirstname =
req.query.firstname;
const safeFirstname =
xssFilters.inHTMLData(unsafeFirstname);
res.send(util.format('<h1>Tom%s</h1>',
safeFirstname)); });
```

SQL Injection

SQL databases are vulnerable to injection attacks where query parameters are exploited to execute arbitrary instructions.

Below is an express framework router that is vulnerable to an SQL injection attack:

```javascript
const express = require('express');
const db = require('./db');

const router = express.Router();

router.get('/email', (req, res) => {
  db.query('SELECT email FROM users WHERE id = ' +
req.query.id);
    .then((record) => {
      // logical flow
      res.send(record[0]);
    })
});
```

In the example above, the application gets user IDs from URLs and retrieves the corresponding email address by querying the database. Two things are wrong in the code snippet.

First, the database query is built using a string concatenation. The second issue is that the user input is concatenated to the query instead of being handled as untrusted data.

An attacker might craft a query string id parameter in such a way that it retrieves all tables or writes into the database. For instance, when the attacker supplies these string parameters:

```
1 UNION SELECT group_concat(table_name) FROM information_schema.tables WHERE table_name = database()
```

This would result to a query like this one:

```
SELECT email FROM users WHERE id = 1 UNION SELECT group_concat(table_name) FROM information_schema.tables WHERE table_name = database()
```

When this query is executed successfully, it would pull the list of all tables in the databases. An attacker can then retrieve any information they want.

To mitigate SQL injections, developers should always perform proper input validation. When input from the user fails the validation checks, the SQL query is not executed.

Another way of preventing SQL injection is using parameterized queries or prepared statements instead of concatenations. Parameterized queries are used to abstract the SQL syntax from the input parameters.

In the example below, a prepared statement, which is Java's implementation of parameterized queries, is used to prevent potential SQL injection attacks.

```
///Wrong implementation

//unvalidated "clientName" parameter appended to the
query allows an attacker to inject any SQL code

String query = "SELECT account_balance FROM user_data
WHERE user_name = "
               + request.getParameter("clientName");
try {
    Statement statement = connection.createStatement(
... );
    ResultSet results = statement.executeQuery( query
);
}


// Correct implementation

String clientname =
request.getParameter("clientName");
// Validate input to detect attacks
String query = "SELECT account_balance FROM user_data
```

Sensitive cookie exposure

The client-side script on every browser can access all the content returned by an application to the server. This includes cookies that often contain sensitive data such as session IDs.

Exposing session identifiers, whether in URLs, error messages, or logs is a bad practice that opens up an application to security issues like cross-site request forgery(CSRF), session hijacking and session fixation.

To prevent this, developers must consistently use HTTPS and implement HTTP-Only cookies. The HTTP-Only attribute in cookies tells the browser to prevent cookie access through the DOM. By doing this, client-side script attacks are prevented from accessing sensitive data stored in cookies.

Another way of securing user sessions is opting by per-requests as opposed to using per-session identifiers. Any time the client requests privileged access permissions, terminate the session and re-authenticate them before granting access.

Here is an example cookie that uses Express – Node.js and stores session data on the SQLite database using the connect-sqlite3 package. Notice how we use HTTP only secure cookies.

```javascript
const express = require('express');
const session = require('express-session');
const SQLiteStore = require('connect-sqlite3')(session);
const util = require('util');

// express-session configuration
const sessionMiddleware = session({
    store: new SQLiteStore({
      table: 'sessions',
      db: 'sessions.db',
      dir: __dirname
    }),
    secret: 'H@rden y0ur c00k1e5',
    saveUninitialized: false,
    resave: false,
    rolling: true,
    name: 'ssid',
    domain: 'localhost',
    httpOnly: true,
    secure: true,
    sameSite: 'strict'
});

const app = express();

// tell Express to use the 'sessionMiddleware'
app.use(sessionMiddleware);

app.get('/', (req, res) => {
  // trigger the 'Set-Cookie' (otherwise no cookie would
be set)
  req.session.counter = (req.session.counter || 0) + 1;

  res.send(util.format('You have ve visited this page
%dtimes',
    req.session.conter));
});

app.listen(4000, () => {
```

Components with known vulnerabilities

There are tons of security risks associated with the use of vulnerable application components. For instance, vulnerabilities in some libraries or other elements such as browser plugin code are a security loophole in your applications.

To ensure the components you're using do not compromise your application's security, always keep up with the current versions of all. Do not rely on unpatched components for building or integrating into your web application.

Another security concern is re-using JavaScript code from open source directories such as GitHub. When you copy code from a random user and re-use it in your application without auditing it, you might introduce security issues in your application.

Instead, exercise caution and inspect every component of your application. You do not want to use any broken code that comes your way, or even worse, code with intentionally malicious scripts.

Putting it all together

Adopting good coding practices can secure applications against common JavaScript vulnerabilities on both the client-side and server-side. When using JavaScript, always follow the following key guidelines for enhanced security:

- Never trust user input
- Use proper encoding/escaping
- Sanitize user input
- Define a content security policy
- Set secure cookies
- Secure API keys on the client-side
- Encrypt data transmitted between the client and the server

- Use secure components and APIs for development
- Use updated libraries and frameworks
- Conduct regular scans on your codebase

Following these best coding practices is usually the first step for securing your web applications.
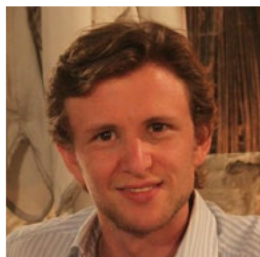
Michael Hollander / About Author

Michael is a Senior Product Manager and the Data Protection Officer at WhiteSource. Before joining WhiteSource, Michael was a Product Manager at GE Digital, and he previously held a number of software development positions spanning over 10 years. Michael is currently leading WhiteSource for Developers, a suite of native developer integrations empowering developers to secure products faster without slowing down development. LinkedIn | Twitter

Recommended Content

AWS S3: Is It Really That Secure?

Wednesday May 4, 2022

Snort, Intrusion Detection, and Unauthorized Use

Thursday April 28, 2022

Open Source Solutions for Cybersecurity Log Management

Monday January 10, 2022
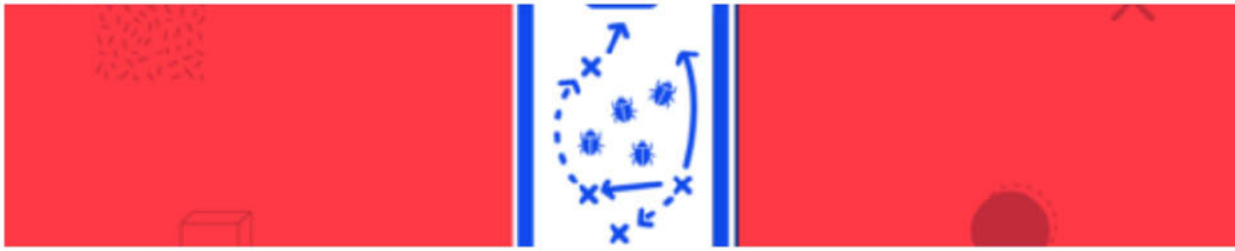
The Use of Playbooks in Vulnerability Management

Thursday December 23, 2021

RESOURCES

Blog

Webinar

Events

SECURE CODING

About Us

Contact Us

Privacy Policy

NEWSLETTER

Enter your email address

SUBSCRIBE

☐ I agree to receive email updates from Secure Coding

JFE Steel Corporation

Prepare for the future with Google Analytics 4

Russell Ketchum

In today's measurement landscape, businesses need to navigate new challenges to understand the complex, multi-platform journeys of their customers — all while prioritizing user privacy.

Two and a half years ago, we [introduced Google Analytics 4](#) to address these evolving measurement standards and help businesses succeed. Google Analytics 4 has the flexibility to measure many different kinds of data, delivering a strong analytics experience that's designed for the future. It allows businesses to see unified user journeys across their websites and apps, use Google's machine learning technology to surface and predict new insights, and most importantly, it's built to keep up with a changing ecosystem.

Without a modern measurement solution, you leave essential insights on the table that can impact your business. So now is the time to make Google Analytics 4 your cross-platform Analytics solution. We will begin sunsetting [Universal Analytics](#) — the previous generation of Analytics — next year. All standard Universal Analytics properties will stop processing new hits on July 1, 2023. Given the new Analytics 360 experience was [recently introduced](#), Universal Analytics 360 properties will receive an additional three months of new hit processing, ending on October 1, 2023.

Moving on from Universal Analytics

Universal Analytics was built for a generation of online measurement that was anchored in the desktop web, independent sessions and more easily observable data from cookies. This measurement methodology is quickly becoming obsolete. Meanwhile, Google Analytics 4 operates across platforms, does not rely exclusively on cookies and uses an event-based data model to deliver user-centric measurement.

And though Universal Analytics offers a variety of privacy controls, Google Analytics 4 is designed with privacy at its core to provide a better experience for both our customers and their users. It helps businesses meet evolving needs and user expectations, with more comprehensive and granular controls for data collection and usage. Importantly, Google Analytics 4 will also no longer store IP addresses. These solutions and controls are especially necessary in today's international data privacy landscape, where users are increasingly expecting more privacy protections and control over their data.

Starting your measurement with Google Analytics 4

Google Analytics 4 is designed with your key objectives in mind — like driving sales or app installs, generating leads or connecting online and offline customer engagement.

Here are just a few ways Google Analytics 4 can support your business.

Understand your customers across touchpoints
Get a complete view of the customer lifecycle with an event-based measurement model that isn't fragmented by platform or organized into independent sessions.

For example, UK-based fitness apparel and accessories brand Gymshark used Google Analytics 4 to

measure across its website and app, allowing the Gymshark team to better understand how users moved through the purchase funnel. As a result, they reduced user drop off by 9%, increased product page clickthroughs by 5% and cut down their own time spent on user journey analysis by 30%.

"Google Analytics 4 was the perfect choice in understanding and improving our new e-commerce app." *Maxwell Petitjean*
Head of Product Insights, Gymshark

Improve ROI with data-driven attribution
Use data-driven attribution to analyze the full impact of your marketing across the customer journey. It assigns attribution credit to more than just the last click using your Analytics data, and helps you understand how your marketing activities collectively influence your conversions. You can export that analysis to Google Ads and Google Marketing Platform media tools to optimize campaigns.

Measure engagement and conversions with business and compliance needs in mind
With new country-level privacy controls, you can manage and minimize the collection of user-level data — like cookies and metadata — while preserving key measurement functionality.

Get greater value from your data
Machine learning generates sophisticated predictive insights about user behavior and conversions, creates new audiences of users likely to purchase or churn and automatically surfaces critical insights to improve your marketing.

Easily activate your insights
Expanded integrations with other Google products, like Google Ads, work across your combined web and app data, making it easy to use Analytics insights to optimize your campaigns.

McDonald's Hong Kong met its goal to grow mobile orders using a predictive audience of "likely seven-day purchasers" and exporting it to Google Ads — increasing app orders more than six times. The team saw a 2.3 times stronger ROI, a 5.6 times increase in revenue, and a 63% reduction in cost per action.

"Google Analytics 4 has equipped us with a strong measurement foundation. We are able to get valuable insights from our first-party data with machine learning and utilize them in our marketing, driving impressive results to future-proof our business."
— Tina Chao, McDonald's Hong Kong Chief Marketing and Digital Customer Experience Officer

And now, Search Ads 360 and Display & Video 360 integrations are available for all customers. This means that any Google Analytics 4 property — standard or 360 — can activate its Analytics data, like conversions and audiences, in Google Marketing Platform buying tools to strengthen campaign performance.

Address your enterprise measurement needs
New sub and roll-up properties in Analytics 360 allow you to customize the structure of your Google Analytics 4 properties to meet data governance needs. This ensures that different teams or partners, like advertising agencies, can access the data they need in accordance with your policies.

Analytics 360 also offers higher limits to meet increasing demand — up to 125 custom dimensions, 400 audiences and 50 conversion types per property. And you'll have peace of mind with service legal agreements (SLAs) across most core functionality, including data collection, processing, reporting and attribution.

"As a large enterprise business with a wide product portfolio, the new Analytics 360 has unlocked insights for our teams to make data-driven decisions, while providing the ability to meet our complex data governance needs with ease and flexibility."
— **Rashi Kacker, Director of Marketing Technology Innovation, Constellation Brands**

What happens next?

All standard Universal Analytics properties will stop processing new hits on July 1, 2023, and 360 Universal Analytics properties will stop processing new hits on October 1, 2023. After that, you'll be able to access your previously processed data in Universal Analytics for at least six months. Learn more about what to expect.

Make the move over to Google Analytics 4 as soon as possible to build the necessary historical data before Universal Analytics stops processing new hits. For guidance, check out our Help Center resources.

≡   **Google**   The Keyword   ⤳ Share   Q

CHROME

More intuitive privacy and security controls in Chrome

May 19, 2020   ·   5 min read   ⤳ Share

A   **AbdelKarim Mardini**
Group Product Manager

Tech > Tech Industry

Default settings for privacy -- we need to talk

"Some assembly required" isn't an effective model for protecting your data.

Alfred Ng 🐦
Dec. 21, 2019 5:00 a.m. PT

6 min read   ↪
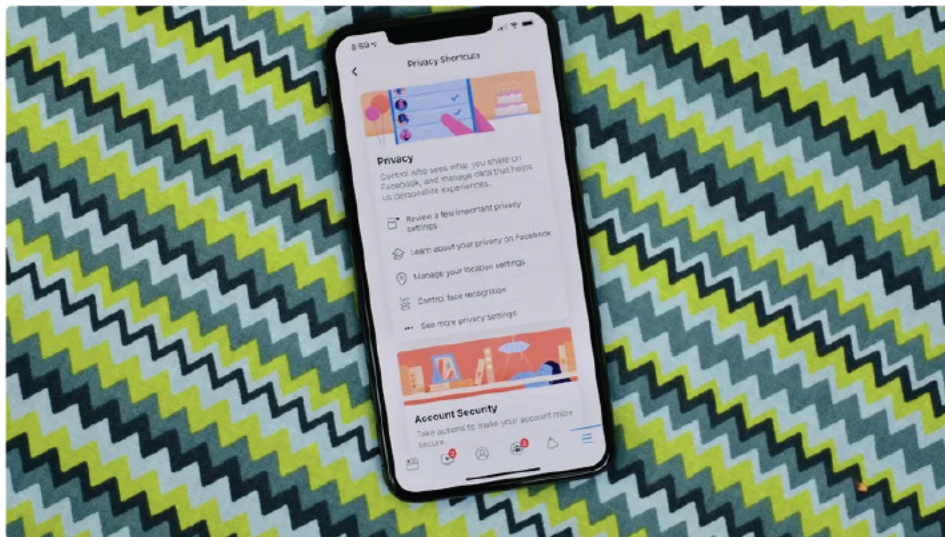
Facebook offers privacy protections, but they're not turned on by default. Industry research shows that the majority of people never change their default settings for privacy.
Jason Cipriani/CNET

When you get a new phone or sign up on a new app, how often do you dig into the privacy settings? If you're like most people, almost never. So while tech giants are giving you more control over privacy, they're counting on you sticking with what you're given.

Over the past couple of years, tech giants have been making changes to privacy settings to give people better options -- whether it's because they've been forced by new laws like California's Consumer Privacy Act or pressure from the public following screw-ups like Facebook's Cambridge Analytica scandal, Amazon's Alexa transcript incidents or Google's location tracking issues.

But if the new privacy protections aren't on by default and people must traverse a maze of clicks to actually get those benefits, then little has actually changed.

CNET has a series of guides on how to change your privacy settings on a number of services and devices -- from smart TVs to voice assistants to online accounts. It begs the question, though: Why does something as fundamental as your own privacy need a guide when billion-dollar companies should be ensuring privacy from the get-go?

Privolta, a company that specializes in privacy-focused ads, ran a study in August and found that it takes 17 clicks to opt out of Google's data collection in the United Kingdom, while it only took one click to give the tech giant consent to collect your data.
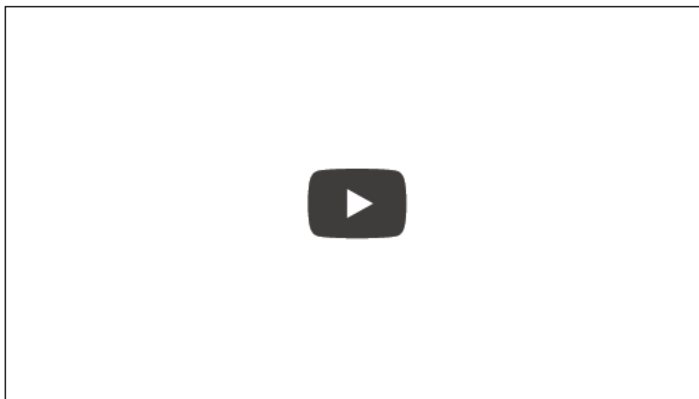
The company looked at 50 of the UK's top websites and found that, on average, it would take five times as long to opt out as it did to opt in for data collection.

"It's designed to wear you down. That's how these patterns work," said Henry Lau, Privolta's co-founder. "They don't want you to make an easy choice between yes and no, they just want you to visit the menu to review your options."

It's not your default

Default settings have a powerful effect on people, even if you have the option to change them at any time.

For comparison, studies have found that organ donation increases in countries where it's the default option. In countries where people must sign up to donate their organs, there's a much lower rate.

The same applies to privacy settings, researchers have found in several studies.

"Several possible reasons for not changing the default settings exist: cognitive and physical laziness; perceiving

Play Sound

Let's talk about why...   00:00 / 00:15
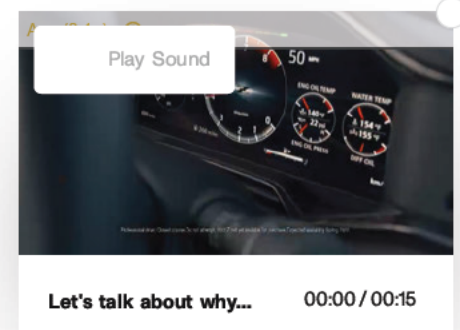
default as correct, perceiving endorsement from the provider; using the default as a justification for choice, lacking transparency of implication, or lacking skill," researchers from the Goethe University Frankfurt and Nelson Mandela Metropolitan University wrote in 2013.

What you get from the tech giants is a decidedly mixed bag. Some recognize that many people don't change default settings and thus turn on privacy protections as the default. Others offer controls, but require people to adjust them. That has a major effect on how much privacy you actually have.

Google's Rick Osterloh tells an audience in New York that its products are built with privacy "at the core," but many of its protections are not turned on by default.

Sarah Tew / CNET

Both Apple and Google say they take privacy seriously and offer controls for data trackers in their respective browsers, Safari and Chrome. The difference is that Safari offers privacy protections by default while Chrome requires people to change their settings.

Less than 10 percent of Safari users but more than 80 percent of Chrome users are tracked by third parties, according to statistics from Gibson Research.

Mozilla, which makes the Firefox browser, started enabling tracking blockers in its browser by default in June. It has blocked more than 1 trillion third-party requests since then, the company said.

"At the baseline, we don't think that people should have to jump through hoops and navigate confusing menus to protect their privacy," said Ashley Boyd, Mozilla's vice president of advocacy. "People are busy, they have a bunch of devices, and it would take a tremendous amount of time for individuals to hunt down their buried settings on each of those to create a private experience."
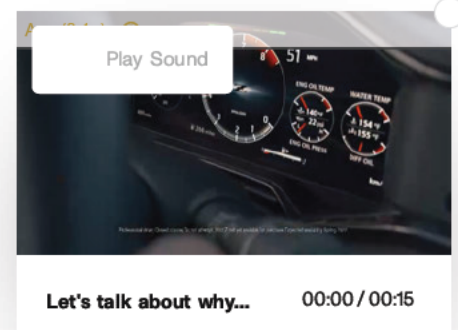
She noted that Mozilla's stance is to shift the burden of protecting privacy from people to tech companies. A handful of tech platforms have followed that model.

When Apple changed its Siri review program, the new default required people to give permission for human reviewers to listen to audio recordings from the digital assistant. Before that, human reviewers listened to a small percentage of people's conversations through Siri in order to help improve the AI.

Google did the same for its voice assistant review program. Amazon's Alexa, however, still requires people to opt out of the review program.

That means your privacy comes by default for Siri and Google Assistant, while it takes six taps and a warning from Amazon to do the same for Alexa.

At Amazon's devices event in September, product chief David Limp boasted that Alexa was the first voice assistant that allowed people to opt out of the listening program -- even though its rivals actually provided better privacy measures.

Amazon declined to provide statistics on how many of its users have opted out of the Alexa listening program. The company explained that it requires users to opt out, rather than matching Apple's and Google's approach, because it believed this was the proper balance between privacy and the need to improve Alexa's artificial intelligence capabilities.

"While we also use unsupervised or semi-supervised learning, supervised learning is still the most effective approach for rapid feature development, accuracy and utility for our customers," an Amazon spokesperson said. "We think this is what customers want with the service, but also want to give them the ability to opt out if they like."

Microsoft leans more toward starting with privacy protections turned off by default, requiring people to alter their settings on their own.

"More than 25 million people around the world – including over 10 million people in the U.S. – have used our privacy dashboard to understand and control their personal data," Microsoft Chief Privacy Officer Julie Brill said in a blog post in November.

The company launched its web-based privacy dashboard in 2017, though the 25 million people who've used it may be a
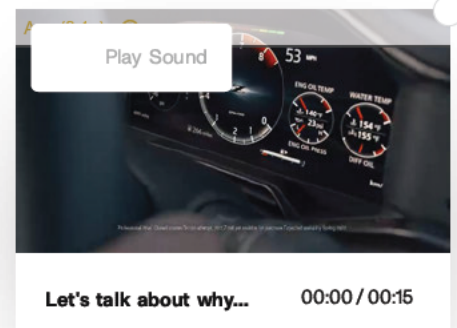
sliver of overall users. The dashboard includes settings for Windows 10, Xbox, Skype, Office, Cortana virtual assistant, Edge web browser, Bing search engine and apps and services. Windows 10 alone runs on more than 900 million devices.

Google didn't provide statistics on how often its users change their privacy settings. Apple also didn't provide statistics on how many people have adjusted their privacy settings. Facebook declined to share data on how often people changed their privacy settings.

Opt in versus opt out

Tech giants have made efforts to educate people about their privacy settings. For example, Facebook hosted a series of privacy pop-ups around the world, where visitors were greeted by staffers who would show them how to access their privacy settings and change their preferences.

The education efforts and pop-ups would be unnecessary if tracking was turned off by default to begin with.

Facebook said that it doesn't offer privacy protections by default because it wants to give people the choice to control their experience on the social network. In focus groups, the company said, it found that people preferred tracking in some cases, noting that participants enjoyed getting relevant ads.

But people would still have that level of control if it were the other way around -- where strict privacy controls were activated by default and people who enjoyed relevant ads could opt in to turn on data tracking.

Amazon hardware chief Dave Limp discusses privacy for its Alexa smart speakers at an event in September. Unlike Siri and Google Assistant, you must opt out of Amazon's human reviews listening program.

James Martin/CNET

Play Sound

Let's talk about why...   00:00 / 00:15
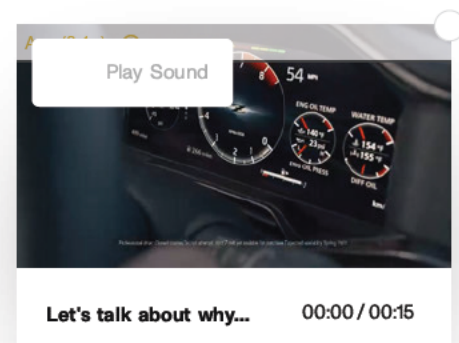
"It's our position that if people value personalization that tracking provides, they can always opt in to it," Mozilla's Boyd said. "Why not shift the balance to allow for personalization for people who want it?"

Mozilla found that when it turned on tracking protections by default, only about 0.5 percent of Firefox users opted in to sharing their data.

Now playing: Let's talk about why privacy settings are a problem   ▶ 4:10
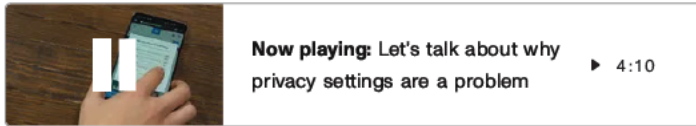
On Jan. 1, 2020, California's Consumer Privacy Act goes into effect, which has already prompted some tech giants to change privacy settings. But a majority of them are still opt-out. For example, the law requires tech companies to provide a "Do Not Sell My Personal Information" link for users in the state, but people must still click on it to get that protection.

There's a growing concern that this protection will be difficult to find on websites because the rules around where the link needs to be displayed haven't been released.

"If it's buried on the site, it effectively neuters the legislation," Privolta's Lau said.

Boyd agreed.

"It feels like a perpetual swimming against the current for most consumers, and that's why default settings are so important for privacy," Boyd said.

Until then, you might want to read our guides about changing your privacy settings.

Play Sound   55

Let's talk about why...   00:00 / 00:15
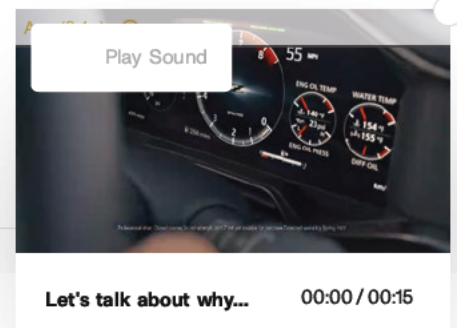
Cookieless Monster:
Exploring the Ecosystem of Web-based Device Fingerprinting

Nick Nikiforakis*, Alexandros Kapravelos[†], Wouter Joosen*, Christopher Kruegel[†], Frank Piessens*, Giovanni Vigna[†]

*iMinds-DistriNet, KU Leuven, 3001 Leuven, Belgium
{firstname.lastname}@cs.kuleuven.be
[†]University of California, Santa Barbara, CA, USA
{kapravel,chris,vigna}@cs.ucsb.edu

Abstract—The web has become an essential part of our society and is currently the main medium of information delivery. Billions of users browse the web on a daily basis, and there are single websites that have reached over one billion user accounts. In this environment, the ability to track users and their online habits can be very lucrative for advertising companies, yet very intrusive for the privacy of users.

In this paper, we examine how web-based device fingerprinting currently works on the Internet. By analyzing the code of three popular browser-fingerprinting code providers, we reveal the techniques that allow websites to track users without the need of client-side identifiers. Among these techniques, we show how current commercial fingerprinting approaches use questionable practices, such as the circumvention of HTTP proxies to discover a user's real IP address and the installation of intrusive browser plugins.

At the same time, we show how fragile the browser ecosystem is against fingerprinting through the use of novel browser-identifying techniques. With so many different vendors involved in browser development, we demonstrate how one can use diversions in the browsers' implementation to distinguish successfully not only the browser-family, but also specific major and minor versions. Browser extensions that help users spoof the user-agent of their browsers are also evaluated. We show that current commercial approaches can bypass the extensions, and, in addition, take advantage of their shortcomings by using them as additional fingerprinting features.

I. INTRODUCTION

In 1994, Lou Montulli, while working for Netscape Communications, introduced the idea of cookies in the context of a web browser [1]. The cookie mechanism allows a web server to store a small amount of data on the computers of visiting users, which is then sent back to the web server upon subsequent requests. Using this mechanism, a website can build and maintain state over the otherwise stateless HTTP protocol. Cookies were quickly embraced by browser vendors and web developers. Today, they are one of the core technologies on which complex, stateful web applications are built.

Shortly after the introduction of cookies, abuses of their stateful nature were observed. Web pages are usually comprised of many different resources, such as HTML, images, JavaScript, and CSS, which can be located both on the web server hosting the main page as well as other third-party web servers. With every request toward a third-party website, that website has the ability to set and read previously-set cookies on a user's browser. For instance, suppose that a user browses to *travel.com*, whose homepage includes a remote image from *tracking.com*. Therefore, as part of the process of rendering *travel.com*'s homepage, the user's browser will request the image from *tracking.com*. The web server of *tracking.com* sends the image along with an HTTP Set-Cookie header, setting a cookie on the user's machine, under the *tracking.com* domain. Later, when the user browses to other websites affiliated with *tracking.com*, e.g., *buy.com*, the tracking website receives its previously-set cookies, recognizes the user, and creates a profile of the user's browsing habits. These *third-party cookies*, due to the adverse effects on a user's privacy and their direct connection with online behavioral advertising, captured the attention of both the research community [2], [3], [4] and the popular media outlets [5] and, ever since, cause the public's discomfort [6], [7].

The user community responded to this privacy threat in multiple ways. A recent cookie-retention study by comScore [8] showed that approximately one in three users delete both first-party and third-party cookies within a month after their visit to a website. Multiple browser-extensions are available that reveal third-party tracking [9], as well as the "hidden" third-party affiliations between sites [10]. In addition, modern browsers now have native support for the rejection of all third-party cookies and some even enable it by default. Lastly, a browser's "Private Mode" is also available to assist users to visit a set of sites without leaving traces of their visit on their machine.

This general unavailability of cookies motivated advertisers and trackers to find new ways of linking users to their browsing histories. Mayer in 2009 [11] and Eckersley in 2010 [12] both showed that the features of a browser and its plugins can be fingerprinted and used to track users without the need of cookies. Today, there is a small number of commercial companies that use such methods to provide *device identification* through web-based fingerprinting. Following the classification of Mowery et al. [13], fingerprinting can be used either constructively or destructively. Constructively,

IEEE computer society

a correctly identified device can be used to combat fraud, e.g., by detecting that a user who is trying to login to a site is likely an attacker who stole a user's credentials or cookies, rather than the legitimate user. Destructively, device identification through fingerprinting can be used to track users between sites, without their knowledge and without a simple way of opting-out. Additionally, device identification can be used by attackers in order to deliver exploits, tailored for specific combinations of browsers, plugins and operating systems [14]. The line between the constructive and destructive use is, however, largely artificial, because the same technology is used in both cases.

Interestingly, companies were offering fingerprinting services as early as 2009, and experts were already voicing concerns over their impact on user privacy [15]. Even when fingerprinting companies honor the recently-proposed "Do Not Track" (DNT) header, the user is still fingerprinted for fraud detection, but the companies *promise* not to use the information for advertising purposes [16]. Note that since the fingerprinting scripts will execute regardless of the DNT value, the verification of this promise is much harder than verifying the effect of DNT on stateful tracking, where the effects are visible at the client-side, in a user's cookies [17].

In this paper, we perform a four-pronged analysis of device identification through web-based fingerprinting. First, we analyze the fingerprinting code of three large, commercial companies. We focus on the differences of their code in comparison to Panopticlick [12], Eckersley's "open-source" implementation of browser fingerprinting. We identify the heavy use of Adobe Flash as a way of retrieving more sensitive information from a client, including the ability to detect HTTP proxies, and the existence of intrusive fingerprinting plugins that users may unknowingly host in their browsers. Second, we measure the adoption of fingerprinting on the Internet and show that, in many cases, sites of dubious nature fingerprint their users, for a variety of purposes. Third, we investigate special JavaScript-accessible browser objects, such as `navigator` and `screen`, and describe novel fingerprinting techniques that can accurately identify a browser even down to its minor version. These techniques involve the ordering of methods and properties, detection of vendor-specific methods, HTML/CSS functionality as well as minor but fingerprintable implementation choices. Lastly, we examine and test browser extensions that are available for users who wish to spoof the identity of their browser and show that, unfortunately *all* fail to completely hide the browser's true identity. This incomplete coverage not only voids the extensions but, ironically, also allows fingerprinting companies to detect the fact that user is attempting to hide, adding extra fingerprintable information.

Our main contributions are:

- We shed light into the current practices of device identification through web-based fingerprinting and propose a taxonomy of fingerprintable information.
- We measure the adoption of fingerprinting on the web.
- We introduce novel browser-fingerprinting techniques that can, in milliseconds, uncover a browser's family and version.
- We demonstrate how over 800,000 users, who are currently utilizing user-agent-spoofing extensions, are more fingerprintable than users who do not attempt to hide their browser's identity, and challenge the advice given by prior research on the use of such extensions as a way of increasing one's privacy [18].

II. Commercial Fingerprinting

While Eckersley showed the principle possibility of fingerprinting a user's browser in order to track users without the need of client-side stateful identifiers [12], we wanted to investigate popular, real-world implementations of fingerprinting and explore their workings. To this end, we analyzed the fingerprinting libraries of three large, commercial companies: BlueCava[1], Iovation[2] and ThreatMetrix[3]. Two of these companies were chosen due to them being mentioned in the web-tracking survey of Mayer and Mitchell [19], while the third one was chosen due to its high ranking on a popular search engine. Given the commercial nature of the companies, in order to analyze the fingerprinting scripts we first needed to discover websites that make use of them. We used Ghostery [9], a browser-extension which lists known third-party tracking libraries on websites, to obtain the list of domains which the three code providers use to serve their fingerprinting scripts. Subsequently, we crawled popular Internet websites, in search for code inclusions, originating from these fingerprinting-owned domains. Once these web sites were discovered, we isolated the fingerprinting code, extracted all individual features, and grouped similar features of each company together.

In this section, we present the results of our analysis, in the form of a taxonomy of possible features that can be acquired through a fingerprinting library. This taxonomy covers all the features described in Panopticlick [12] as well as the features used by the three studied fingerprinting companies. Table I lists all our categories and discovered features, together with the method used to acquire each feature. The categories proposed in our taxonomy resulted by viewing a user's fingerprintable surface as belonging to a layered system, where the "application layer" is the browser and any fingerprintable in-browser information. At the top of this taxonomy, scripts seek to fingerprint and identify any browser customizations that the user has directly or indirectly performed. In lower levels, the scripts target user-specific information around the browser, the operating system and even the hardware and network of a user's

[1] http://www.bluecava.com
[2] http://www.iovation.com
[3] http://www.threatmetrix.com

542

Fingerprinting Category	Panopticlick	BlueCava	Iovation ReputationManager	ThreatMetrix
Browser customizations	Plugin enumeration$_{(JS)}$ Mime-type enumeration$_{(JS)}$ ActiveX + 8 CLSIDs$_{(JS)}$	Plugin enumeration$_{(JS)}$ ActiveX + 53 CLSIDs$_{(JS)}$ Google Gears Detection$_{(JS)}$		Plugin enumeration$_{(JS)}$ Mime-type enumeration$_{(JS)}$ ActiveX + 6 CLSIDs$_{(JS)}$ Flash Manufacturer$_{(FLASH)}$
Browser-level user configurations	Cookies enabled$_{(HTTP)}$ Timezone$_{(JS)}$ Flash enabled$_{(JS)}$	System/Browser/User Language$_{(JS)}$ Timezone$_{(JS)}$ Flash enabled$_{(JS)}$ Do-Not-Track User Choice$_{(JS)}$ MSIE Security Policy$_{(JS)}$	Browser Language$_{(HTTP, JS)}$ Timezone$_{(JS)}$ Flash enabled$_{(JS)}$ Date & time$_{(JS)}$ Proxy Detection$_{(FLASH)}$	Browser Language$_{(FLASH)}$ Timezone$_{(JS, FLASH)}$ Flash enabled$_{(JS)}$ Proxy Detection$_{(FLASH)}$
Browser family & version	User-agent$_{(HTTP)}$ ACCEPT-Header$_{(HTTP)}$ Partial S.Cookie test$_{(JS)}$	User-agent$_{(JS)}$ Math constants$_{(JS)}$ AJAX Implementation$_{(JS)}$	User-agent$_{(HTTP, JS)}$	User-agent$_{(JS)}$
Operating System & Applications	User-agent$_{(HTTP)}$ Font Detection$_{(FLASH, JAVA)}$	User-agent$_{(JS)}$ Font Detection$_{(JS, FLASH)}$ Windows Registry$_{(SFP)}$	User-agent$_{(HTTP, JS)}$ Windows Registry$_{(SFP)}$ MSIE Product key$_{(SFP)}$	User-agent$_{(JS)}$ Font Detection$_{(FLASH)}$ OS+Kernel version$_{(FLASH)}$
Hardware & Network	Screen Resolution$_{(JS)}$	Screen Resolution$_{(JS)}$ Driver Enumeration$_{(SFP)}$ IP Address$_{(HTTP)}$ TCP/IP Parameters$_{(SFP)}$	Screen Resolution$_{(JS)}$ Device Identifiers$_{(SFP)}$ TCP/IP Parameters$_{(SFP)}$	Screen Resolution$_{(JS, FLASH)}$

Table I

TAXONOMY OF ALL FEATURES USED BY PANOPTICLICK AND THE STUDIED FINGERPRINTING PROVIDERS - SHADED FEATURES ARE, IN COMPARISON TO PANOPTICLICK, EITHER SUFFICIENTLY EXTENDED, OR ACQUIRED THROUGH A DIFFERENT METHOD, OR ENTIRELY NEW

machine. In the rest of this section, we focus on all the non-trivial techniques used by the studied fingerprinting providers that were not previously described in Eckersley's Panopticlick [12].

A. Fingerprinting through popular plugins

As one can see in Table I, all companies use Flash, in addition to JavaScript, to fingerprint a user's environment. Adobe Flash is a proprietary browser plug-in that has enjoyed wide adoption among users, since it provided ways of delivering rich media content that could not traditionally be displayed using HTML. Despite the fact that Flash has been criticized for poor performance, lack of stability, and that newer technologies, like HTML5, can potentially deliver what used to be possible only through Flash, it is still available on the vast majority of desktops.

We were surprised to discover that although Flash reimplements certain APIs existing in the browser and accessible through JavaScript, its APIs do not always provide the same results compared to the browser-equivalent functions. For instance, for a Linux user running Firefox on a 64-bit machine, when querying a browser about the platform of execution, Firefox reports "Linux x86_64". Flash, on the other hand, provides the full kernel version, e.g., Linux 3.2.0-26-generic. This additional information is not only undesirable from a privacy perspective, but also from a security perspective, since a malicious web-server could launch an attack tailored not only to a browser and architecture but to a specific kernel. Another API call that behaves differently is the one that reports the user's screen resolution. In the Linux implementations of the Flash plugin (both Adobe's and Google's), when a user utilizes a dual-monitor setup, Flash reports as the width of a screen the sum of the two individual screens. This value, when combined with the browser's response (which lists the resolution of the monitor were the browser-window is located), allows a fingerprinting service to detect the presence of multiple-monitor setups.

Somewhat surprisingly, none of the three studied fingerprinting companies utilized Java. One of them had some dead code that revealed that in the past it probably did make use of Java, however, the function was not called anymore and the applet was no longer present on the hard-coded location listed in the script. This is an interesting deviation from Panopticlick, which did use Java as an alternate way of obtaining system fonts. We consider it likely that the companies abandoned Java due to its low market penetration in browsers. This, in turn, is most likely caused by the fact that many have advised the removal of the Java plugin from a user's browser [20], [21] due to the plethora of serious Java vulnerabilities that were discovered and exploited over the last few years.

B. Vendor-specific fingerprinting

Another significant difference between the code we analyzed and Panopticlick is that, the fingerprinting companies were not trying to operate in the same way across all browsers. For instance, when recognizing a browser as Internet Explorer, they would extensively fingerprint Internet-Explorer-specific properties, such as `navigator.securityPolicy` and `navigator.systemLanguage`. At the same time, the code accounted for the browser's "short-comings," such as using a lengthy list of predefined CLSIDs for Browser-Helper-Objects (BHOs) due to Internet Explorer's unwillingness to enumerate its plugins.

543

Listing 1 Side-channel inference of the presence or absence of a font

```
function get_text_dimensions(font){

  h = document.getElementsByTagName("BODY")[0];
  d = document.createElement("DIV");
  s = document.createElement("SPAN");

  d.appendChild(s);
  d.style.fontFamily = font;
  s.style.fontFamily = font;
  s.style.fontSize = "72px";
  s.innerHTML = "font_detection";
  h.appendChild(d);

  textWidth = s.offsetWidth;
  textHeight = s.offsetHeight;
  h.removeChild(d);

  return [textWidth, textHeight];
}
```

Font Family	String	Width x Height
Sans	font_detection	519x84
Arial	font detection	452x83
Calibri	font detection	416x83

Figure 1.   The same string, rendered with different fonts, and its effects on the string's width and height, as reported by the Google Chrome browser

C. Detection of fonts

The system's list of fonts can serve as part of a user's unique fingerprint [12]. While a browser does not directly provide that list, one can acquire it using either a browser plugin that willingly provides this information or using a side-channel that indirectly reveals the presence or absence of any given font.

1) Plugin-based detection: ActionScript, the scripting language of Flash, provides APIs that include methods for discovering the list of fonts installed on a running system. While this traditionally was meant to be used as a way of ensuring the correct appearance of text by the plugin, it can also be used to fingerprint the system. Two out of the three studied companies were utilizing Flash as a way of discovering which fonts were installed on a user's computer. Interestingly, only one of the companies was preserving the order of the font-list, which points, most likely, to the fact that the other is unaware that the order of fonts is stable and machine-specific (and can thus be used as an extra fingerprinting feature).

2) Side-channel inference: The JavaScript code of one of the three fingerprinting companies included a fall-back method for font-detection, in the cases where the Flash plugin was unavailable. By analyzing that method, we discovered that they were using a technique, similar to the CSS history stealing technique [22], to identify the presence or absence of any given font - see Listing 1.

More precisely, the code first creates a `<div>` element. Inside this element, the code then creates a `<span>` element with a predetermined text string and size, using a provided font family. Using the `offsetWidth` and

`offsetHeight` methods of HTML elements, the script discovers the layout width and height of the element. This code is first called with a "sans" parameter, the font typically used by browsers as a fall-back, when another requested font is unavailable on a user's system. Once the height and text for "sans" are discovered, another script goes over a pre-defined list of fonts, calling the `get_text_dimensions` function for each one. For any given font, if the current width or height values are different from the ones obtained through the original "sans" measurement, this means that the font does exist and was used to render the predefined text. The text and its size are always kept constant, so that if its width or height change, this change will only be due to the different font. Figure 1 shows three renderings of the same text, with the same font-size but different font faces in Google Chrome. In order to capitalize as much as possible on small differences between fonts, the font-size is always large, so that even the smallest of details in each individual letter will add up to measurable total difference in the text's height and width. If the height and width are identical to the original measurement, this means that the requested font did not exist on the current system and thus, the browser has selected the sans fall-back font. All of the above process, happens in an invisible iframe created and controlled by the fingerprinting script and thus completely hidden from the user.

Using this method, a fingerprinting script can rapidly discover, even for a long list of fonts, those that are present on the operating system. The downside of this approach is that less popular fonts may not be detected, and that the font-order is no longer a fingerprintable feature.

D. Detection of HTTP Proxies

One of the features that are the hardest to spoof for a client is its IP address. Given the nature of the TCP protocol, a host cannot pretend to be listening at an IP address from which it cannot reliably send and receive packets. Thus, to hide a user's IP address, another networked machine (a proxy) is typically employed that relays packets between the user that wishes to remain hidden and a third-party. In the context of browsers, the most common type of proxies are HTTP proxies, through which users configure their browsers to send all requests. In addition to manual configuration, browser plugins are also available that allow for a more controlled use of remote proxies, such as the automatic routing of different requests to different proxies based on
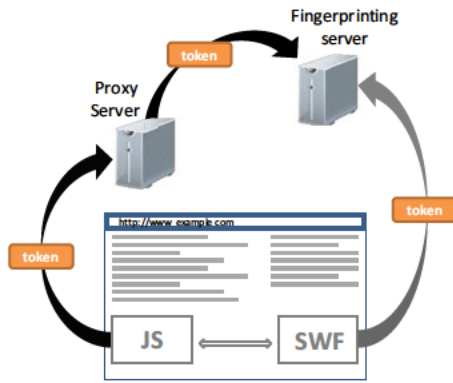
544

Figure 2.   Fingerprinting libraries take advantage of Flash's ability to ignore browser-defined HTTP proxies to detect the real IP address of a user

pattern matching of each request[4], or the cycling of proxies from a proxy list at user-defined intervals[5].

From the point of view of device identification through fingerprinting, a specific IP address is an important feature. Assuming the use of fingerprinting for the detection of fraudulent activities, the distinction between a user who is situated in a specific country and one that *pretends* to be situated in that country, is crucial. Thus, it is in the interest of the fingerprint provider to detect a user's real IP address or, at least, discover that the user is utilizing a proxy server.

When analyzing the ActionScript code embedded in the SWF files of two of the three fingerprinting companies, we found evidence that the code was circumventing the user-set proxies at the level of the browser, i.e., the loaded Flash application was contacting a remote host directly, disregarding any browser-set HTTP proxies. We verified this behavior by employing both an HTTP proxy and a packet-capturing application, and noticing that certain requests were captured by the latter but were never received by the former. In the code of both of the fingerprinting companies, certain long alphanumerical tokens were exchanged between JavaScript and Flash and then used in their communication to the server. While we do not have access to the server-side code of the fingerprinting providers, we assume that the identifiers are used to correlate two possibly different IP addresses. In essence, as shown in Figure 2, if a JavaScript-originating request contains the same token as a Flash-originating request from a different source IP address, the server can be certain that the user is utilizing an HTTP proxy.

Flash's ability to circumvent HTTP proxies is a somewhat known issue among privacy-conscious users that has lead to the disabling of Flash in anonymity-providing applications, like TorButton [23]. Our analysis shows that it is actively exploited to identify and bypass web proxies.

[4]FoxyProxy - http://getfoxyproxy.org/
[5]ProxySwitcher - http://www.proxyswitcher.com/

E. System-fingerprinting plugins

Previous research on fingerprinting a user's browser focused on the use of popular browser plugins, such as Flash and Java, and utilized as much of their API surface as possible to obtain user-specific data [11], [12]. However, while analyzing the plugin-detection code of the studied fingerprinting providers, we noticed that two out of the three were searching a user's browser for the presence of a special plugin, which, if detected, would be loaded and then invoked. We were able to identify that the plugins were essentially native fingerprinting libraries, which are distributed as CAB files for Internet Explorer and eventually load as DLLs inside the browser. These plugins can reach a user's system, either by a user accepting their installation through an ActiveX dialogue, or bundled with applications that users download on their machines. DLLs are triggered by JavaScript through ActiveX, but they run natively on the user's machine, and thus can gather as much information as the Internet Explorer process.

We downloaded both plugins, wrapped each DLL into an executable that simply hands-off control to the main routine in the DLL and submitted both executables to Anubis [24], a dynamic malware analysis platform that executes submitted binaries in a controlled environment. We focused on the Windows registry values that were read by the plugin, since the registry is a rich environment for fingerprinting. The submitted fingerprinting DLLs were reading a plethora of system-specific values, such as the hard disk's identifier, TCP/IP parameters, the computer's name, Internet Explorer's product identifier, the installation date of Windows, the Windows Digital Product Id and the installed system drivers – entries marked with SFP in Table I.

All of these values combined provide a much stronger fingerprint than what JavaScript or Flash could ever construct. It is also worthwhile mentioning that one of the two plugins was misleadingly identifying itself as "Reputation-Shield" when asking the user whether she wants to accept its installation. Moreover, none of 44 antivirus engines of VirusTotal [25] identified the two DLLs as malicious, even though they clearly belong to the *spyware* category. Using identifiers found within one DLL, we were also able to locate a Patent Application for Iovation's fingerprinting plugin that provides further information on the fingerprinting process and the gathered data [26].

F. Fingerprint Delivery Mechanism

In the fingerprinting experiments of Mayer [11] and Eckersley [12], there was a 1-to-1 relationship between the page conducting the fingerprinting and the backend storing the results. For commercial fingerprinting, however, there is a N-to-1 relationship, since each company provides fingerprinting services to many websites (through the inclusion of third-party scripts) and needs to obtain user fingerprints from each of these sites. Thus, the way that the fingerprint and

545

the information about it are delivered is inherently different from the two aforementioned experiments.

Through our code analysis, we found two different scenarios of fingerprinting. In the first scenario, the first-party site was not involved in the fingerprinting process. The fingerprinting code was delivered by an advertising syndicator, and the resulting fingerprint was sent back to the fingerprinting company. This was most likely done to combat click-fraud, and it is unclear whether the first-party site is even aware of the fact that its users are being fingerprinted.

In the second scenario, where the first-party website is the one requesting the fingerprint, we saw that two out of the three companies were adding the final fingerprint of the user into the DOM of the hosting page. For instance, `www.imvu.com` is using BlueCava for device fingerprinting by including remote scripts hosted on BlueCava's servers. When BlueCava's scripts combine all features into a single fingerprint, the fingerprint is DES-encrypted (DES keys generated on the fly and then encrypted with a public key), concatenated with the encrypted keys and finally converted to Base64 encoding. The resulting string is added into the DOM of `www.imvu.com`; more precisely, as a new hidden input element in IMVU's login form. In this way, when the user submits her username and password, the fingerprint is also sent to IMVU's web servers. Note, however, that IMVU cannot decrypt the fingerprint and must thus submit it back to BlueCava, which will then reply with a "trustworthiness" score and other device information. This architecture allows BlueCava to hide the implementation details from its clients and to correlate user profiles across its entire client-base. Iovation's fingerprinting scripts operate in a similar manner.

Constrastingly, ThreatMetrix delivers information about users in a different way. The including site, i.e., a customer of ThreatMetrix, creates a session identifier that it places into a `<div>` element with a predefined identifier. ThreatMetrix's scripts, upon loading, read this session identifier and append it to all requests towards the ThreatMetrix servers. This means that the including site never gets access to a user's fingerprint, but only information about the user by querying ThreatMetrix for specific session identifiers.

G. Analysis Limitations

In the previous sections we analyzed the workings of the fingerprinting libraries of three popular commercial companies. The analysis was a mostly manual, time-consuming process, where each piece of code was gradually deobfuscated until the purpose of all functions was clear. Given the time required to fully reverse-engineer each library, we had to limit ourselves to analyze the script of each fingerprinting company as it was seen through two different sites (that is, two different clients of each company). However, we cannot exclude the possibility of additional scripts that are present on the companies' web servers that would perform more operations than the ones we encountered.

III. ADOPTION OF FINGERPRINTING

In Section II, we analyzed the workings of three commercial fingerprinting companies and focused on the differences of their implementations when compared to Panopticlick [12]. In this section, we study the fingerprinting ecosystem, from the point of view of websites that leverage fingerprinting.

A. Adoption on the popular web

To quantify the use of web-based fingerprinting on popular websites, we crawled up to 20 pages for each of the Alexa top 10,000 sites, searching for script inclusions and iframes originating from the domains that the three studied companies utilize to serve their fingerprinting code. To categorize the discovered domains, we made use of the publicly-available domain categorization service of TrendMicro [6], a popular anti-virus vendor.

Through this process, we discovered 40 sites (0.4% of the Alexa top 10,000) utilizing fingerprinting code from the three commercial providers. The most popular site making use of fingerprinting is *skype.com*, while the two most popular categories of sites are: "Pornography" (15%) and "Personals/Dating" (12.5%). For pornographic sites, a reasonable explanation is that fingerprinting is used to detect shared or stolen credentials of paying members, while for dating sites to ensure that attackers do not create multiple profiles for social-engineering purposes. Our findings show that fingerprinting is already part of some of the most popular sites of the Internet, and thus the hundreds of thousands of their visitors are fingerprinted on a daily basis.

Note that the aforementioned adoption numbers are lower bounds since our results do not include pages of the 10,000 sites that were not crawled, either because they were behind a registration wall, or because they were not in the set of 20 URLs for each crawled website. Moreover, some popular sites may be using their own fingerprinting algorithms for performing device identification and not rely on the three studied fingerprinting companies.

B. Adoption by other sites

To discover less popular sites making use of fingerprinting, we used a list of 3,804 domains of sites that, when analyzed by Wepawet [27], requested the previously identified fingerprinting scripts.

Each domain was submitted to TrendMicro's and McAfee's categorization services [7] which provided as output the domain's category and "safety" score. We used two categorizing services in an effort to reduce, as much as possible, the number of "untested" results, i.e., the number of websites not analyzed and not categorized. By examining the results, we extracted as many popular categories as possible

---

[6]TrendMicro - http://global.sitesafety.trendmicro.com/
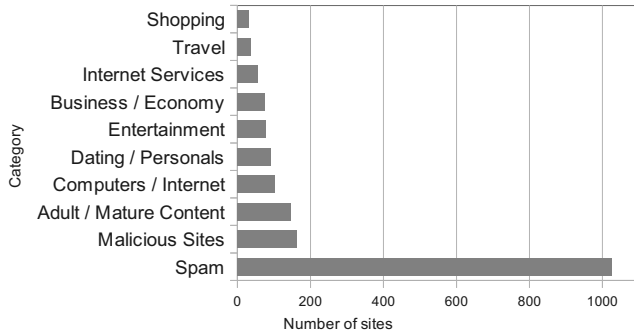[7]McAfee - http://mcafee.com/threat-intelligence/domain/

Figure 3.   The top 10 categories of websites utilizing fingerprinting

and created aliases for names that were referring to the same category, such as "News / Media" versus "General News" and "Disease Vector" versus "Malicious Site". If a domain was characterized as "dangerous" by one, and "not dangerous" by the other, we accepted the categorization of the latter, so as to give the benefit of the doubt to legitimate websites that could have been compromised, when the former service categorized it.

Given the use of two domain-categorization services, a small number of domains (7.9%) was assigned conflicting categories, such as "Dating" versus "Adult/Mature" and "Business/Economy" versus "Software/Hardware." For these domains, we accepted the characterization of McAfee, which we observed to be more precise than TrendMicro's for less popular domains. Excluding 40.8% of domains which were reported as "untested" by both services, the results of this categorization are shown in Figure 3.

First, one can observe that eight out of the ten categories, include sites which operate with user subscriptions, many of which contain personal and possibly financial information. These sites are usually interested in identifying fraudulent activities and the hijacking of user accounts. The Adult/Mature category seems to make the most use of fingerprinting as was the case with the Alexa top 10,000 sites.

The top two categories are also the ones that were the least expected. 163 websites were identified as malicious, such as using exploits for vulnerable browsers, conducting phishing attacks or extracting private data from users, whereas 1,063 sites were categorized as "Spam" by the two categorizing engines. By visiting some sites belonging to these categories, we noticed that many of them are parked webpages, i.e., they do not hold any content except advertising the availability of the domain name, and thus do not currently include fingerprinting code. We were however able to locate many "quiz/survey" sites that are, at the time of this writing, including fingerprinting code from one of the three studied companies. Visitors of these sites are greeted with a "Congratulations" message, which informs them that they have won and asks them to proceed to receive their prize. At some

later step, these sites extract a user's personal details and try to subscribe the user to expensive mobile services.

While our data-set is inherently skewed towards "maliciousness" due to its source, it is important to point out that all of these sites were found to include, at some point in time, fingerprinting code provided by the three studied providers. This observation, coupled with the fact that for all three companies, an interested client must set an appointment with a sales representative in order to acquire fingerprinting services, point to the possibility of fingerprinting companies working together with sites of dubious nature, possibly for the expansion of their fingerprint databases and the acquisition of more user data.

IV.   FINGERPRINTING THE BEHAVIOR OF SPECIAL OBJECTS

In Section II, we studied how commercial companies perform their fingerprinting and created a taxonomy of fingerprintable information accessible through a user's browser. In Table I, one can notice that, while fingerprinting companies go to great lengths to discover information about a browser's plugins and the machine hosting the browser, they mostly rely on the browser to willingly reveal its true identity (as revealed through the `navigator.userAgent` property and the User-Agent HTTP header). A browser's user-agent is an important part of a system's fingerprint [18], and thus it may seem reasonable to assume that if users modify these default values, they will increase their privacy by hiding more effectively from these companies.

In this section, however, we demonstrate how fragile the browser ecosystem is against fingerprinting. Fundamental design choices and differences between browser types are used in an effort to show how difficult it can be to limit the exposure of a browser to fingerprinting. Even different versions of the same browser can have differences in the scripting environment that identify the browser's real family, version, and, occasionally, even the operating system. In the rest of this section we describe several novel browser-identifying techniques that: a) can complement current fingerprinting, and b) are difficult to eliminate given the current architecture of web browsers.

A.   Experimental Fingerprinting Setup

Our novel fingerprinting techniques focus on the special, browser-populated JavaScript objects; more precisely, the `navigator` and `screen` objects. Contrary to objects created and queried by a page's JavaScript code, these objects contain vendor- and environment-specific methods and properties, and are thus the best candidates for uncovering vendor-specific behaviors.

To identify differences between browser-vendors and to explore whether these differences are consistent among installations of the same browser on multiple systems, we constructed a fingerprinting script that performed a series of

"everyday" operations on these two special objects (such as adding a new property to an object, or modifying an existing one) and reported the results to a server. In this and the following section, we describe the operations of our fingerprinting script and our results. Our constructed page included a JavaScript program that performed the following operations:

1) Enumerated the `navigator` and `screen` object, i.e., request the listing of all properties of the afore-mentioned objects.
2) Enumerated the `navigator` object again, to ensure that the order of enumeration does not change.
3) Created a custom object, populated it, and enumerated it. A custom, JavaScript-created object, allows us to compare the behavior of browser-populated objects (such as `navigator`) with the behavior of "classic" JavaScript objects.
4) Attempted to delete a property of the `navigator` object, the `screen` object, and the custom object.
5) Add the possibly-deleted properties back to their objects.
6) Attempted to modify an existing property of the `navigator` and `screen` objects.
7) If `Object.defineProperty` is implemented in the current browser, utilize it to make an existing property in the `navigator`, `screen`, and custom object non-enumerable.
8) Attempt to delete the `navigator` and `screen` objects.
9) Attempt to assign new custom objects to the `navigator` and `screen` variable names.

At each step, the objects involved were re-enumerated, and the resulting data was Base64-encoded and sent to our server for later processing. Thus, at the server side, we could detect whether a property was deleted or modified, by comparing the results of the original enumeration with the current one. The enumeration of each object was conducted through code that made use of the *prop in obj* construct, to avoid forcing a specific order of enumeration of the objects, allowing the engine to list object properties in the way of its choosing.

B. Results

By sharing the link to our fingerprinting site with friends and colleagues, we were able, within a week, to gather data from 68 different browsers installations, of popular browsers on all modern operating systems. While our data is small in comparison to previous studies [11], [12], we are not using it to draw conclusions that have statistical relevance but rather, as explained in the following sections, to find deviations between browsers and to establish the consistency of these deviations. We were able to identify the following novel ways of distinguishing between browsers:

Order of enumeration: Through the analysis of the output from the first three steps of our fingerprinting algorithm (Sec. IV-A), we discovered that the order of property-enumeration of special browser objects, like the `navigator` and `screen` objects, is consistently different between browser families, versions of each browser, and, in some cases, among deployments of the same version on different operating systems. While in the rest of this section we focus to the `navigator` object, the same principles apply to the `screen` object.

Our analysis was conducted in the following manner. After grouping the `navigator` objects and their enumerated properties based on browser families, we located the `navigator` object with the least number of properties. This version was consistently belonging to the oldest version of a browser, since newer versions add new properties which correspond to new browser features, such as the `navigator.doNotTrack` property in the newer versions of Mozilla Firefox. The order of the properties of this object, became our baseline to which we compared the `navigator` objects of all subsequent versions of the same browser family. To account for ordering changes due to the introduction of new properties in the `navigator` object, we simply excluded all properties that were not part of our original baseline object, without however changing the relative order of the rest of the properties. For instance, assume an ordered set of features B, where $B_0 = \{a, b, c, d\}$ and $B_1 = \{a, b, \underline{e}, c, d, \underline{f}\}$. B_1 has two new elements in comparison with B_0, namely e and f which, however, can be removed from the set without disrupting the relative order of the rest. For every browser version within the same browser-family, we compared the `navigator` object to the baseline, by first recording and removing new features and then noting whether the order of the remaining features was different from the order of the baseline.

The results of this procedure are summarized in Table II. For each browser family, we compare the ordering of the `navigator` object among up to five different versions. The most current version is denoted as V_c. The first observation is that in almost 20 versions of browsers, no two were ever sharing the same order of properties in the `navigator` object. This feature by itself, is sufficient to categorize a browser to its correct family, regardless of any property-spoofing that the browser may be employing. Second, all browsers except Chrome maintain the ordering of `navigator` elements between versions. Even when new properties were introduced, these do not alter the relative order of all other properties. For instance, even though the newest version of Mozilla Firefox (V_c) has 7 extra features when compared to the oldest version (V_{c-4}), if we ignore these features then the ordering is the same with the original ordering (W).

Google Chrome was the only browser that did not exhibit this behavior. By analyzing our dataset, we discovered that

548

Browser	V_{c-4}	V_{c-3}	V_{c-2}	V_{c-1}	V_c
Mozilla Firefox	W	W+1	W+4	W+5	W+7
Microsoft IE	-	-	X	X	X+1
Opera	Y	Y+1	Y+1	Y+3	Y+5
Google Chrome	Z	Z	Z'+1	Z''+1	Z'''+1

Table II
DIFFERENCES IN THE ORDER OF `NAVIGATOR` OBJECTS BETWEEN
VERSIONS OF THE SAME BROWSER

Browser	Unique methods & properties
Mozilla Firefox	screen.mozBrightness screen.mozEnabled navigator.mozSms + 10
Google Chrome	navigator.webkitStartActivity navigator.getStorageUpdates
Opera	navigator.browserLanguage navigator.getUserMedia
Microsoft IE	screen.logicalXDPI screen.fontSmoothingEnabled navigator.appMinorVersion +11

Table III
UNIQUE METHODS AND PROPERTIES OF THE `NAVIGATOR` AND `SCREEN`
OBJECTS OF THE FOUR MAJOR BROWSER-FAMILIES

Chrome not only changed the order between subsequent versions of the browser, but also between deployments of the same browser on different operating systems. For instance, Google Chrome v.20.0.1132.57 installed on Mac OSX has a different order of elements than the same version installed on a Linux operating system. In Table II, we compare the order of properties of the `navigator` object when the underlying OS is Windows XP. While this changing order may initially appear to be less-problematic than the stable order of other browsers, in reality, the different orderings can be leveraged to detect a specific version of Google Chrome, and, in addition, the operating system on which the browser is running.

Overall, we discovered that the property ordering of special objects, such as the `navigator` object, is consistent among runs of the same browser and runs of the same version of browsers on different operating systems. Contrastingly, the order of properties of a custom script-created object (Step 3 in Section IV-A) was identical among all the studied browsers even though, according to the ECMAScript specification, objects are *unordered* collections of properties [28] and thus the exact ordering can be implementation-specific. More precisely, the property ordering of the custom objects was always the same with the order of property creation.

In general, the browser-specific, distinct property ordering of special objects can be directly used to create models of browsers and, thus, unmask the real identity of a browser. Our findings are in par with the "order-matters" observation made by previous research: Mayer discovered that the list of plugins as reported by browsers was ordered based on the installation time of each individual plugin [11]. Eckersley noticed that the list of fonts, as reported by Adobe Flash and Sun's Java VM, remained stable across visits of the same user [12].

Unique features: During the first browser wars in the mid-90s, browser vendors were constantly adding new features to their products, with the hope that developers would start using them. As a result, users would have to use a specific browser, effectively creating a browser lock-in [29]. The features ranged from new HTML tags to embedded scripting languages and third-party plugins. Signs of this "browser battle" are still visible in the contents of the user-agent string of modern browsers [30].

Today, even though the HTML standard is governed by the W3C committee and JavaScript by Ecma International, browser vendors still add new features that do not belong to any specific standard. While these features can be leveraged by web developers to provide users with a richer experience, they can also be used to differentiate a browser from another. Using the data gathered by our fingerprinting script, we isolated features that were available in only one family of browsers, but not in any other. These unique features are summarized in Table III. All browser families had at least two such features that were not shared by any other browser. In many cases, the names of the new features were starting with a vendor-specific prefix, such as `screen.`mozBrightness for Mozilla Firefox and `navigator.`msDoNotTrack for Microsoft Internet Explorer. This is because browser-vendors are typically allowed to use prefixes for features not belonging to a standard or not yet standardized [31]. In the context of fingerprinting, a script can query for the presence or absence of these unique features (e.g., typeof screen.mozBrightness != "undefined") to be certain of the identity of any given browser.

An interesting sidenote is that these unique features can be used to expose the real version of Mozilla Firefox browser, even when the user is using the Torbutton extension. Torbutton replaces the `navigator` and `screen` objects with its own versions, spoofing the values of certain properties, so as to protect the privacy of the user [32]. We installed Torbutton on Mozilla Firefox version 14 and, by enumerating the `navigator` object, we observed that, among others, the Torbutton had replaced the `navigator.userAgent` property with the equivalent of Mozilla Firefox version 10, and it was claiming that our platform was Windows instead of Linux. At the same time, however, special Firefox-specific properties that Mozilla introduced in versions 11 to 14 of Firefox (such as `navigator.mozBattery` and `navigator.mozSms`)

were still available in the `navigator` object. These discrepancies, combined with other weaknesses found in less thorough user-agent-spoofing extensions (see Section V), can uncover not only that the user is trying to hide, but also that she is using Torbutton to do so.

Mutability of special objects: In the two previous sections, we discussed the ability to exploit the enumeration-order and unique features of browsers for fingerprinting. In this section, we investigate whether each browser treats the `navigator` and `screen` objects like regular JavaScript objects. More precisely, we investigate whether these objects are mutable, i.e., whether a script can delete a specific property from them, replace a property with a new one, or delete the whole object. By comparing the outputs of steps four to nine from our fingerprinting algorithm, we made the following observations.

Among the four browser families, only Google Chrome allows a script to delete a property from the `navigator` object. In all other cases, while the "delete" call returns successfully and no exceptions are thrown, the properties remain present in the special object. When our script attempted to modify the value of a property of `navigator`, Google Chrome and Opera allowed it, while Mozilla Firefox and Internet Explorer ignored the request. In the same way, these two families were the only ones allowing a script to reassign `navigator` and `screen` to new objects. Interestingly, no browser allowed the script to simply delete the `navigator` or `screen` object. Finally, Mozilla Firefox behaved in a unique way when requested to make a certain property of the `navigator` object non-enumerable. Specifically, instead of just hiding the property, Firefox behaved as if it had actually deleted it, i.e., it was no longer accessible even when requested by name.

Evolution of functionality: Recently, we have seen a tremendous innovation in Web technologies. The competition is fierce in the browsers' scene, and vendors are trying hard to adopt new technologies and provide a better platform for web applications. Based on that observation, in this section, we examine if we can determine a browser's version based on the new functionality that it introduces. We chose Google Chrome as our testing browser and created a library in JavaScript that tests if specific functionality is implemented by the browser. The features that we selected to capture different functionality were inspired by web design compatibility tests (where web developers verify if their web application is compatible with a specific browser). In total, we chose 187 features to test in 202 different versions of Google Chrome, spanning from version *1.0.154.59* up to *22.0.1229.8*, which we downloaded from *oldapps.com* and which covered all 22 major versions of Chrome. We found that not all of the 187 features were useful; only 109 actually changed during Google Chrome's evolution. These browser
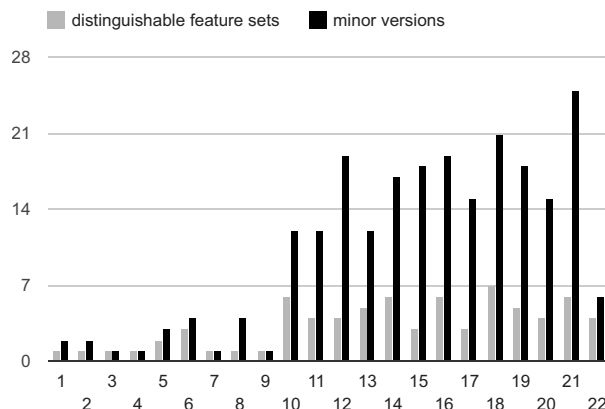
Figure 4.   A comparison between how many distinguishable feature sets and minor Google Chrome versions we have per Google Chrome's major versions.

versions covered not only releases from the stable channel of Google Chrome, but also from Beta and Dev channels. We refer to a major version as the first number of Google Chrome's versioning system, and to minor version as the full number of the version. We used a virtual machine with Windows XP to setup all browser versions, and used all versions to visit our functionality-fingerprinting page.

In total, we found 71 sets of features that can be used to identify a specific version of Google Chrome. Each feature set could identify versions that range from a single Google Chrome version up to 14 different versions. The 14 Chrome versions that were sharing the same feature set were all part of the *12.0.742.** releases. Among all 71 sets, there were only four cases where the same feature set was identifying more than a single major version of the browser. In all of these cases, the features overlapped with the first Dev release of the next major version, while subsequent releases from that point on had different features implemented. In Figure 4, we show how many minor versions of Chrome we examined per major version and how many distinct feature sets we found for each major version. The results show that we can not only identify the major version, but in most cases, we have several different feature sets on the same major version. This makes the identification of the exact browser version even more fine-grained.

In Figure 5, we show how one can distinguish all Google Chrome's major versions by checking for specific features. Every pair of major versions is separated by a feature that was introduced into the newer version and did not exist in the previous one. Thus, if anyone wants to distinguish between two consecutive versions, a check of a single feature is sufficient to do so. Notice that our results indicate that we can perform even more fine-grained version detection than the major version of Google Chrome (we had 71 distinct sets of enabled features compared to 22 versions of Chrome), but for simplicity we examined only
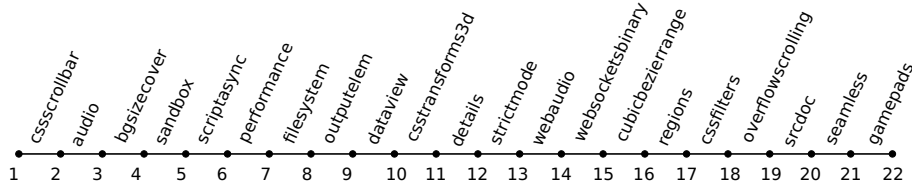
550

Figure 5.   Feature-based fingerprinting to distinguish between Google Chrome major versions

the major version feature changes in detail.

Miscellaneous: In this section, we list additional browser-specific behaviors that were uncovered through our experiment but that do not fall in the previous categories.

Our enumeration of object-properties indirectly uses the method `toString()` for the examined objects. By comparing the formatted output of some specific properties and methods, we noticed that different browsers treated them in slightly different ways. For instance, when calling `toString()` on the natively implemented `navigator.javaEnabled` method, browsers simply state that it is a "native function." Although all the examined browser families print "function javaEnabled() { [native code] }," Firefox uses newline characters after the opening curly-bracket and before the closing one. Interestingly, Internet Explorer does not list the `navigator.javaEnabled` when requested to enumerate the `navigator` object, but still provides the "native function" print-out when asked specifically about the `javaEnabled` method. In the same spirit, when our scripts invoked the `toString()` method on the `navigator.plugins` object, Google Chrome reported "[object DOMPluginArray]," Internet Explorer reported "[object]," while both Mozilla Firefox and Opera reported "[object PluginArray]."

Lastly, while trying out our fingerprinting page with various browsers, we discovered that Internet Explorer lacks native support for Base64 encoding and decoding (`atob` and `btoa`, respectively) which our script used to encode data before sending them to the server.

C. Summary

Overall, one can see how various implementation choices, either major ones, such as the traversal algorithms for JavaScript objects and the development of new features, or minor ones, such as the presence or absence of a newline character, can reveal the true nature of a browser and its JavaScript engine.

V. ANALYSIS OF USER-AGENT-SPOOFING EXTENSIONS

With the advent of browser add-ons, many developers have created extensions that can increase the security of users (e.g., extensions showing HTML forms with non-secure destinations) or their privacy (e.g., blocking known ads and web-tracking scripts).

Extension	#Installations	User Rating
Mozilla Firefox		
UserAgent Switcher	604,349	4/5
UserAgent RG	23,245	4/5
UAControl	11,044	4/5
UserAgentUpdater	5,648	3/5
Masking Agent	2,262	4/5
User Agent Quick Switch	2,157	5/5
randomUserAgent	1,657	4/5
Override User Agent	1,138	3/5
Google Chrome		
User-Agent Switcher for Chrome	123,133	4/5
User-Agent Switcher	21,108	3.5/5
Ultimate User Agent Switcher, URL sniffer	28,623	4/5

Table IV
LIST OF USER-AGENT-SPOOFING BROWSER EXTENSIONS

In the context of this paper, we were interested in studying the completeness and robustness of extensions that attempt to hide the true nature of a browser from an inspecting website. As shown in Table I, while the studied companies do attempt to fingerprint a user's browser customizations, they currently focus only on browser-plugins and do not attempt to discover any installed browser-extensions. Given however the sustained popularity of browser-extensions [33], we consider it likely that fingerprinting extensions will be the logical next step. Note that, unlike browser plugins, extensions are not enumerable through JavaScript and, thus, can only be detected through their side-effects. For instance, some sites currently detect the use of Adblock Plus [34] by searching for the absence of specific iframes and DOM elements that are normally created by advertising scripts.

Since a browser exposes its identity through the user-agent field (available both as an HTTP header and as a property of the JavaScript-accessible `navigator` object), we focused on extensions that advertised themselves as capable of spoofing a browser's user agent. These extensions usually serve two purposes. First, they allow users to surf to websites that impose strict browser requirements onto their visitors, without fulfilling these requirements. For instance, some sites are developed and tested using one specific browser and, due to the importance of the content loading correctly, refuse to load on other browsers. Using a user-agent-spoofing extension, a user can visit such a site, by pretending to use one of the white-listed browsers.

551

	Google Chrome	Mozilla Firefox	MSIE	Opera
navigator.product	Gecko	Gecko	N/A	N/A
navigator.appCodeName	Mozilla	Mozilla	Mozilla	Mozilla
navigator.appName	Netscape	Netscape	Microsoft Internet Explorer	Opera
navigator.platform	Linux i686	Linux x86_64	Win32	Linux
navigator.vendor	Google Inc.	(empty string)	N/A	N/A

Table V
STANDARD PROPERTIES OF THE NAVIGATOR OBJECT AND THEIR
VALUES ACROSS DIFFERENT BROWSER FAMILIES

Another reason for using these extensions is to protect the privacy of a user. Eckeresly, while gathering data for the Panopticlick project, discovered that there were users whose browsers were reporting impossible configurations, for instance, a device was pretending to be an iPhone, but at the same time had Adobe Flash support. In that case, these were users who were obviously trying to get a non-unique browser fingerprint by Panopticlick. Since Eckersley's study showed the viability of using common browser features as parts of a unique fingerprint, it is reasonable to expect that legitimate users utilize such extensions to reduce the trackability of their online activities, even if the extensions' authors never anticipated such a use. Recently, Trusteer discovered in an "underground" forum a spoofing-guide that provided step-by-step instructions for cybercriminals who wished to fool fraud-detection mechanisms that used device-fingerprinting [35]. Among other advice, the reader was instructed to download an extension that changes the User-Agent of their browser to make their sessions appear as if they were originating by different computers with different browsers and operating systems.

Table IV shows the Mozilla Firefox and Google Chrome extensions that we downloaded and tested, together with their user base (measured in July 2012) and the rating that their users had provided. The extensions were discovered by visiting each market, searching for "user-agent" and then downloading all the relevant extensions with a sufficiently large user base and an above-average rating. A high rating is important because it indicates the user's satisfaction in the extension fulfilling its purpose. Our testing consisted of listing the `navigator` and `screen` objects through JavaScript and inspecting the HTTP headers sent with browser requests, while the extensions were actively spoofing the identity of the browser. As in Section IV, we chose to focus on these two objects since they are the ones that are the most vendor-specific as well as the most probed by the fingerprinting libraries. Through our analysis, we discovered that, unfortunately, in *all* cases, the extensions were inadequately hiding the real identity of the browser, which could still be straightforwardly exposed through JavaScript. Apart from being vulnerable to every fingerprinting technique that we introduced in Section IV, each extension had one or more of the following issues:

- **Incomplete coverage of the navigator object.** In many cases, while an extension was modifying the `navigator.userAgent` property, it would leave intact other revealing properties of the navigator object, such as `appName`, `appVersion` and `vendor` - Table V. Moreover, the extensions usually left the `navigator.platform` property intact, which allowed for improbable scenarios, like a Microsoft Internet Explorer browser running on Linux.
- **Impossible configurations.** None of the studied extensions attempted to alter the `screen` object. Thus, users who were utilizing laptops or normal workstations and pretended to be mobile devices, were reporting impossible screen width and height (e.g., a reported 1920x1080 resolution for an iPhone).
- **Mismatch between User-agent values.** As discussed earlier, the user-agent of any given browser is accessible through the HTTP headers of a browser request and through the userAgent property of the `navigator` object. We found that some extensions would change the HTTP headers of the browser, but not of the `navigator` object. Two out of three Chrome extensions were presenting this behavior.

We want to stress that these extensions are not malicious in nature. They are legitimately-written software that unfortunately did not account for all possible ways of discovering the true identity of the browsers on which they are installed. The downside here is that, not only fingerprinting libraries can potentially detect the actual identity of a browser, thus, undermining the goals of the extension, but also that they can discover the discrepancies between the values reported by the extensions and the values reported by the browser, and then use these differences as extra features of their fingerprints. The discrepancies of each specific extension can be modeled and thus, as with Adblock Plus, used to uncover the presence of specific extensions, through their side-effects.

The presence of any user-agent-spoofing extension is a discriminatory feature, under the assumption that the majority of browsing users are not familiar enough with privacy threats (with the possible exception of cookies) to install such spoofing extensions. As a rough metric, consider that the most popular extension for Mozilla Firefox is Adblock Plus [34] that, at the time of this writing, is installed by fifteen million users, 25 times more users than UserAgent Switcher, the most popular extension in Table IV.

We characterize the extension-problem as an *iatrogenic* [8] one. The users who install these extensions in an effort

---

[8]*iatrogenic* - Of or relating to illness caused by medical examination or treatment.

552

to hide themselves in a crowd of popular browsers, install software that actually makes them more visible and more distinguishable from the rest of the users, who are using their browsers without modifications. As a result, we advice against the use of user-agent-spoofing extensions as a way of increasing one's privacy. Our findings come in direct antithesis with the advice given by Yen et al. [18], who suggest that user-agent-spoofing extensions *can* be used, as a way of making tracking harder. Even though their study focuses on common identifiers as reported by client-side HTTP headers and the client's IP address, a server capable of viewing these can respond with JavaScript code that will uncover the user-agent-spoofing extension, using any of the aforementioned techniques.

VI. DISCUSSION

Given the intrusive nature of web-based device fingerprinting and the current inability of browser extensions to actually enhance a user's privacy, in this section, we first discuss possible ways of reducing a user's fingerprintable surface and then briefly describe alternative uses of fingerprinting which may become more prevalent in the future.

A. Reducing the fingerprintable surface

Flash. As described in Section II, Adobe Flash was utilized by all three fingerprinting libraries that we studied, due to its rich API that allow SWF files to access information not traditionally available through a browser's API. In all cases, the SWF file responsible for gathering information from the host was hidden from the user, by either setting the width and height of the `<object>` tag to zero, or placed into an iframe of zero height and width. In other words, there was no visible change on the web page that included the fingerprinting SWF files. This observation can be used as a first line of defense. All modern browsers have extensions that disallow Flash and Silverlight to be loaded until explicitly requested by the user (e.g., through a click on the object itself). These hidden files cannot be clicked on and thus, will never execute. While this is a straightforward solution that would effectively stop the Flash-part of the fingerprint of all three studied companies, a circumvention of this countermeasure is possible. By wrapping their fingerprinting code into an object of the first-party site and making that object desirable or necessary for the page's functionality, the fingerprinting companies can still execute their code. This, however, requires much more integration between a first-party website and a third-party fingerprinting company than the current model of "one-size-fits-all" JavaScript and Flash.

In the long run, the best solution against fingerprinting through Flash should come directly from Flash. In the past, researchers discovered that Flash's Local Shared Objects, i.e., Flash's equivalent of browser cookies, were not deleted when a user exited her browser's private mode or even when she used the "Clear Private Data" option of her browser's UI [36]. As a result, in the latest version of Flash, LSOs are not stored to disk but simply kept in memory when the browser's private mode is utilized [37]. Similarly, when a browser enters private mode, Flash could provide less system information, respect any browser-set HTTP proxies and possibly report only a standard subset of a system's fonts, to protect a user's environment from fingerprinting.

JavaScript. There are multiple vendors involved in the development of JavaScript engines, and every major browser is equipped with a different engine. To unify the behavior of JavaScript under different browsers, all vendors would need to agree not only on a single set of API calls to expose to the web applications, but also to internal implementation specifics. For example, hash table implementations may affect the order of objects in the exposed data structures of JavaScript, something that can be used to fingerprint the engine's type and version. Such a consensus is difficult to achieve among all browser vendors, and we have seen diversions in the exposed APIs of JavaScript even in the names of functions that offer the same functionality, e.g., `execScript` and `eval`. Also, based on the fact that the vendors *battle* for best performance of their JavaScript engines, they might be reluctant to follow specific design choices that might affect performance.

At the same time, however, browsers could agree to sacrifice performance when "private-mode" is enabled, where there could be an attempt to expose a unified interface.

B. Alternative uses of fingerprinting

Although, in this paper, we have mostly focused on fingerprinting as a fraud-detection and web-tracking mechanism, there is another aspect that requires attention. Drive-by downloads and web attacks in general use fingerprinting to understand if the browser that they are executing on is vulnerable to one of the multiple available exploits. This way, the attackers can decide, at the server-side, which exploit to *reveal* to the client, exposing as little as they can of their attack capabilities. There are three different architectures to detect drive-by downloads: low-interaction honeypots, high-interaction honeypots and honeyclients. In all three cases, the browser is either a specially crafted one, so that it can instrument the pages visited, or a browser installation that was never used by a real user. Given the precise, browser-revealing, fingerprinting techniques that we described in this paper, it is possible to see in the future these mechanisms being used by attackers to detect monitoring environments and circumvent detection.

VII. RELATED WORK

To the best of our knowledge, this paper is the first that attempts to study the problem of web-based fingerprinting from the perspectives of all the players involved, i.e., from the perspective of the fingerprinting providers and their

fingerprinting methods, the sites utilizing fingerprinting, the users who employ privacy-preserving extensions to combat fingerprinting, and the browser's internals and how they relate to its identity.

Eckersley conducted the first large-scale study showing that various properties of a user's browser and plugins can be combined to form a unique fingerprint [12]. More precisely, Eckersley found that from about 500,000 users who visited `panopticlick.eff.org` and had Flash or Java enabled, 94.2% could be uniquely identified, i.e., there was no other user whose environment produced the same fingerprint. His study, and surprisingly accurate identification results, prompted us to investigate commercial fingerprinting companies and their approach. Yen et al. [18] performed a fingerprinting study, similar to Eckersley's, by analyzing month-long logs of Bing and Hotmail. Interestingly, the authors utilize a client's IP address as part of their tracking mechanism, which Eckersley explicitly avoids dismissing it as "not sufficiently stable." As a way of protecting oneself, the authors advocated the use of user-agent-spoofing extensions. As we discussed in Section V, this is actually counter-productive since it allows for more fingerprinting rather than less.

Mowery et al. [13] proposed the use of benchmark execution time as a way of fingerprinting JavaScript implementations, under the assumption that specific versions of JavaScript engines will perform in a consistent way. Each browser executes a set of predefined JavaScript benchmarks, and the completion-time of each benchmark forms a part of the browser's performance signature. While their method correctly detects a browser-family (e.g., Chrome) 98.2% of the time, it requires over three minutes to fully execute. According to a study conducted by Alenty [38], the average view-time of a web page is 33 seconds. This means that, with high likelihood, the benchmarks will not be able to completely execute and thus, a browser may be misclassified. Moreover, the reported detection rate of more specific attributes, such as the browser-version, operating system and architecture, is significantly less accurate.

Mowery and Shacham later proposed the use of rendering text and WebGL scenes to a `<canvas>` element as another way of fingerprinting browsers [39]. Different browsers will display text and graphics in a different way, which, however small, can be used to differentiate and track users between page loads. While this method is significantly faster than the execution of browser benchmarks, these technologies are only available in the latest versions of modern browsers, thus they cannot be used to track users with older versions. Contrastingly, the fingerprinting techniques introduced in Section IV can be used to differentiate browsers and their versions for any past version.

Olejnik et al. [40] show that web history can also be used as a way of fingerprinting without the need of additional client-side state. The authors make this observation

by analyzing a corpus of data from when the CSS-visited history bug was still present in browsers. Today, however, all modern browsers have corrected this issue and thus, extraction of a user's history is not as straightforward, especially without user interaction [41]. Olejnik et al. claim that large script providers, like Google, can use their near-ubiquitous presence to extract a user's history. While this is true [42], most users have first-party relationships with Google, meaning that they can be tracked accurately, without the need of resorting to history-based fingerprinting.

VIII. CONCLUSION

In this paper, we first investigated the real-life implementations of fingerprinting libraries, as deployed by three popular commercial companies. We focused on their differences when compared to Panopticlick and discovered increased use of Flash, backup solutions for when Flash is absent, broad use of Internet Explorer's special features, and the existence of intrusive system-fingerprinting plugins.

Second, we created our own fingerprinting script, using multiple novel features that mainly focused on the differences between special objects, like the `navigator` and `screen`, as implemented and handled by different browsers. We identified that each browser deviated from all the rest in a consistent and measurable way, allowing scripts to almost instantaneously discover the true nature of a browser, regardless of a browser's attempts to hide it. To this end, we also analyzed eleven popular user-agent spoofing extensions and showed that, even without our newly proposed fingerprinting techniques, all of them fall short of properly hiding a browser's identity.

The purpose of our research was to demonstrate that when considering device identification through fingerprinting, user-privacy is currently on the losing side. Given the complexity of fully hiding the true nature of a browser, we believe that this can be efficiently done only by the browser vendors. Regardless of their complexity and sophistication, browser-plugins and extensions will never be able to control everything that a browser vendor can. At the same time, it is currently unclear whether browser vendors would desire to hide the nature of their browsers, thus the discussion of web-based device fingerprinting, its implications and possible countermeasures against it, must start at a policy-making level in the same way that stateful user-tracking is currently discussed.

REFERENCES

[1] The New York Times - John Schwartz, "Giving the Web a Memory Cost Its Users Privacy," http://www.nytimes.com/2001/09/04/technology/04COOK.html.

[2] B. Krishnamurthy, "Privacy leakage on the Internet," presented at IETF 77, March 2010.

[3] B. Krishnamurthy and C. E. Wills, "Generating a privacy footprint on the Internet," in *Proceedings of the 6th ACM SIGCOMM Conference on Internet Measurement*, ser. IMC '06, New York, NY, USA, 2006, pp. 65–70.

[4] F. Roesner, T. Kohno, and D. Wetherall, "Detecting and defending against third-party tracking on the web," in *NSDI'12: Proceedings of the 9th USENIX conference on Networked Systems Design and Implementation*.   Berkeley, CA, USA: USENIX Association, 2012, pp. 12–12.

[5] The Wall Street Journal, "What They Know," http://blogs.wsj.com/wtk/.

[6] J. Turow, J. King, C. J. Hoofnagle, A. Bleakley, and M. Hennessy, "Americans Reject Tailored Advertising and Three Activities that Enable It," 2009.

[7] B. Ur, P. G. Leon, L. F. Cranor, R. Shay, and Y. Wang, "Smart, useful, scary, creepy: perceptions of online behavioral advertising," in *Proceedings of the Eighth Symposium on Usable Privacy and Security*, ser. SOUPS '12.   New York, NY, USA: ACM, 2012, pp. 4:1–4:15.

[8] comScore, "The Impact of Cookie Deletion on Site-Server and Ad-Server Metrics in Australia," January 2011.

[9] "Ghostery," http:wwww.ghostery.com.

[10] "Collusion: Discover who's tracking you online," http://www.mozilla.org/en-US/collusion/.

[11] J. R. Mayer, "Any person... a pamphleteer," Senior Thesis, Stanford University, 2009.

[12] P. Eckersley, "How Unique Is Your Browser?" in *Proceedings of the 10th Privacy Enhancing Technologies Symposium (PETS)*, 2010.

[13] K. Mowery, D. Bogenreif, S. Yilek, and H. Shacham, "Fingerprinting information in JavaScript implementations," in *Proceedings of W2SP 2011*, H. Wang, Ed.   IEEE Computer Society, May 2011.

[14] C. Kolbitsch, B. Livshits, B. Zorn, and C. Seifert, "Rozzle: De-cloaking internet malware," in *IEEE Symposium on Security and Privacy*, May 2012.

[15] E. Mills, "Device identification in online banking is privacy threat, expert says," CNET News (April 2009).

[16] "Opt out of being tracked," http://www.bluecava.com/preferences/.

[17] J. R. Mayer, "Tracking the Trackers: Early Results — Center for Internet and Society," http://cyberlaw.stanford.edu/node/6694.

[18] T.-F. Yen, Y. Xie, F. Yu, R. P. Yu, and M. Abadi, "Host Fingerprinting and Tracking on the Web: Privacy and Security Implications," in *Proceddings of the 19th Annual Network and Distributed System Security Symposium (NDSS)*, 2012.

[19] J. R. Mayer and J. C. Mitchell, "Third-party web tracking: Policy and technology," in *IEEE Symposium on Security and Privacy*, 2012, pp. 413–427.

[20] G. Cluley, "How to turn off Java on your browser - and why you should do it now," http://nakedsecurity.sophos.com/2012/08/30/how-turn-off-java-browser/.

[21] B. Krebs, "How to Unplug Java from the Browser," http://krebsonsecurity.com/how-to-unplug-java-from-the-browser.

[22] D. Jang, R. Jhala, S. Lerner, and H. Shacham, "An empirical study of privacy-violating information flows in JavaScript Web applications," in *Proceedings of CCS 2010*, Oct. 2010.

[23] "Torbutton: I can't view videos on YouTube and other flash-based sites. Why?" https://www.torproject.org/torbutton/torbutton-faq.html.en#noflash.

[24] "Anubis: Analyzing Unknown Binaries," http://anubis.iseclab.org/.

[25] "VirusTotal - Free Online Virus, Malware and URL Scanner," https://www.virustotal.com/.

[26] G. Pierson and J. DeHaan, "Patent US20080040802 - NETWORK SECURITY AND FRAUD DETECTION SYSTEM AND METHOD."

[27] M. Cova, C. Kruegel, and G. Vigna, "Detection and analysis of drive-by-download attacks and malicious javascript code," in *Proceedings of the 19th International Conference on World Wide Web (WWW)*, 2010, pp. 281–290.

[28] "ECMAScript Language Specification, Standard ECMA-262, Third edition."

[29] M. Zalewski, *The Tangled Web: A Guide to Securing Modern Web Applications*.   No Starch Press, 2011.

[30] A. Andersen, "History of the browser user-agent string," http://webaim.org/blog/user-agent-string-history.

[31] "Web Tracking Protection," http://www.w3.org/Submission/2011/SUBM-web-tracking-protection-20110224/.

[32] P. Eckersley, "Panopticlick — Self-Defense," https://panopticlick.eff.org/self-defense.php.

[33] J. Scott, "How many Firefox users have add-ons installed? 85%!" https://blog.mozilla.org/addons/2011/06/21/firefox-4-add-on-users/.

[34] "Adblock plus - for annoyance-free web surfing," http://adblockplus.org.

[35] A. Klein, "How Fraudsters are Disguising PCs to Fool Device Fingerprinting," http://www.trusteer.com/blog/how-fraudsters-are-disguising-pcs-fool-device-fingerprinting.

[36] A. Soltani, S. Canty, Q. Mayo, L. Thomas, and C. J. Hoofnagle, "Flash Cookies and Privacy," in *SSRN preprint (August 2009)*.

[37] J. Xu and T. Nguyen, "Private browsing and Flash Player 10.1," http://www.adobe.com/devnet/flashplayer/articles/privacy_mode_fp10_1.html.

[38] J.-L. Gassée and F. Filloux, "Measuring Time Spent On A Web Page," http://www.cbsnews.com/2100-215_162-5037448.html.

[39] K. Mowery and H. Shacham, "Pixel perfect: Fingerprinting canvas in HTML5," in *Proceedings of W2SP 2012*, M. Fredrikson, Ed.   IEEE Computer Society, May 2012.

[40] Ł. Olejnik, C. Castelluccia, and A. Janc, "Why Johnny Can't Browse in Peace: On the Uniqueness of Web Browsing History Patterns," in *the 5th workshop on Hot Topics in Privacy Enhancing Technologies (HOTPETS 2012)*.

[41] Z. Weinberg, E. Y. Chen, P. R. Jayaraman, and C. Jackson, "I still know what you visited last summer: Leaking browsing history via user interaction and side channel attacks," in *Proceedings of the 2011 IEEE Symposium on Security and Privacy*, ser. SP '11, 2011, pp. 147–161.

[42] N. Nikiforakis, L. Invernizzi, A. Kapravelos, S. V. Acker, W. Joosen, C. Kruegel, F. Piessens, and G. Vigna, "You Are What You Include: Large-scale Evaluation of Remote JavaScript Inclusions," in *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, 2012.

Oxford English Dictionary | The definitive record of the English language

private, *adj.1, adv.*, and *n.*

Pronunciation: ⓘ Brit.   /ˈprʌɪvɪt/, U.S.   /ˈpraɪvɪt/

Forms: ...

Frequency (in current use):

Origin: A borrowing from Latin. **Etymons:** Latin *prīvātus, prīvātum, privata.*

Etymology: < classical Latin *prīvātus...*

A. *adj.1*
I. Restricted to one person or a few persons as opposed to the wider community; largely in opposition to *public.*

†**1.** Of a religious rule: not shared by all Christians. Of an individual or a religious order: living according to distinct religious rules; set apart by distinct beliefs, religious practices, etc. *Obsolete.*

> Applied by Wyclif to the mendicant orders (Franciscans, Augustines, Dominicans, and Carmelites).

> ‣ 1395   *Remonstr. against Romish Corruptions* (Titus) in *Eng. Hist. Rev.* (1911) **26** 747 (*MED*)   Religiouse possessioneris..shulden ben apaied wiþ scars liflode & cloþinge geten wiþ here owne labour bi here privat rule [L. *secundum eorum regulam*], which þei seyn þat seynt benet & seynt austin maden to suche religiouse men.

> a1425   J. WYCLIF *Sel. Eng. Wks.* (1869) I. 67 (*MED*)   Þis asse and hir fole ben comen to þes pryvat ordris but not to alle Cristene men.

> c1475 (‣ c1445)   R. PECOCK *Donet* (1921) 79   Al priuate religiosite stondiþ in keping of þre vowis..vowe of chastite, vowe of wilful pouerte..and vowe of obedience to her prelate.

2.

a. Restricted to or for the use or enjoyment of one particular person or group of people; not open to the public.

> Now frequently on a sign or notice indicating this (see, e.g., quot. a1911).

> ‣ a1398   J. TREVISA tr. Bartholomaeus Anglicus *De Proprietatibus Rerum* (BL Add.) f. 332   Þe priuate wey longiþ to nyȝe towne and is schort and nyȝ and ofte ygrowe wiþ gras.

> ?a1475 (‣ ?a1425)   tr. R. Higden *Polychron.* (Harl. 2261) (1865) I. 91 (*MED*)   The seruauntes goe on foote..to commune festes and priuate [a1387 J. Trevisa tr. priue] offices.

> a1600 (‣ 1535)   W. STEWART tr. H. Boece *Bk. Cron. Scotl.* (1858) II. 63   Quhair he wes bureit in ane prevat place.

> 1623   W. SHAKESPEARE & J. FLETCHER *Henry VIII* III. i. 28   May it please you Noble Madam, to withdraw Into your priuate Chamber.

> 1638   R. BRATHWAIT *Bessie Bell* in *Barnabees Journall* (new ed.) sig. Ee2   This place it is private.

> 1696   *Earl of Galloway's Family Papers* 6 Aug.   Wee..did meet at a privat countrey ale house.

> 1759   S. JOHNSON *Prince of Abissinia* I. i. 2   According to the custom.., he [*sc.* Rasselas] was confined in a

private palace.

1817   W. Selwyn *Abridgem. Law Nisi Prius* (ed. 4) II. 1242   A person having a private way over the land of another, cannot, when the way is become impassable by the overflowing of a river, justify going on the adjoining land.

1849   T. B. Macaulay *Hist. Eng.* II. vi. 142   News which reached him through private channels.

1862   W. Sandby *Hist. Royal Acad. Arts* II. 239   It had..been the custom to regard the anniversary dinner as one of a private nature—a gathering of the members of the Royal Academy and of the friends and patrons of art.

*a*1911   D. G. Phillips *Susan Lenox* (1917) II. xi. 285   A man strode toward the frosted glass door marked 'Private'.

1992   *Daily Star* 16 Jan. 15/2   A drugs squad detective..has been suspended after claims that a cannabis joint was rolled at a private party.

b. Of or relating to a service provided on a paying basis, as opposed to through the State or another public body (sometimes with implication of benefit to an individual as distinct from a group).

(a) Of, relating to, or designating teaching or other educational facilities provided on an individual basis, or for which fees are charged.

Chiefly in compounds.

In British use, *private* schools were originally contrasted with *public* schools which, while also charging fees, were run as charitable institutions for the benefit of the public, while private schools were run for the personal profit of the proprietors; this distinction was subsequently lost.

1574   E. Hake *Touchestone Time Present* sig. F3   Now tell me whether priuate schoole or publicke better is.

1574   E. Hake *Touchestone Time Present* sig. O^v   But if the publique care Should happe to cease, then euery man at home must needes prepare To haue a priuate teacher.

1581   R. Mulcaster *Positions* xl. 228   If the maister minde his boorders eitheer only or most, where his charge is ouer moe, where then is his dutie? if not, what gaine haue those boorders, by their maisters priuate?

1581   R. Mulcaster *Positions* xxxix. 183 (*heading*)   Of priuate and publike education, with their generall goods & illes.

1670   D. Lloyd *State Worthies* (ed. 2) 402   When private Tutors had initiated, publick Schools had seasoned, and the University had improved this Gentlemans sprightly and noble parts.

1695   J. Bellers *Proposals Raising Colledge Industry* 18   And I think such a Colledge-Education, under good Rules, beyond any Private one, having several Advantages the Private will want.

1756   M. Calderwood *Lett. & Jrnls.* (1884) vi. 153   As for the boys of fashion,..if they are come from the country, they are boarded in what they call a *pension*, or have a private tutor to teach them.

1792   M. Wollstonecraft *Vindic. Rights Woman* xii. 361   The good effects resulting from attention to private education will ever be very confined, and the parent who really puts his own hand to the plow, will always, in some degree, be disappointed.

1848   G. Moberly *Winchester Serm.* II. Pref.   What then..is a public school? and wherein does it essentially differ from a private one?

1875   A. Trollope *Prime Minister* (1876) I. i. 6   He had been at a good English private school.

1999   *Financial Times* 9 Oct. (FT 1,000 Schools Suppl.) 3/3   Several schools, including the five King Edward VI grammar schools in the West Midlands, have raised the prospect of 'going private' if local parents vote to abolish the 11-plus.

(b) Of, relating to, or designating medical treatment or facilities for which fees are charged to the patient instead of being provided by the State or a public body; *spec.* (in the United Kingdom since 1948) designating medical treatment or facilities outside the National Health Service.

> 1754   W. Smellie *Treat. Midwifery* II. xxvi. 437   I attended a private patient.
>
> 1826   *Lancet* 5 Aug. 599/2   Many cases..to increase the revenue of some private practitioner.
>
> 1859   F. Nightingale *Notes on Nursing* vi. 38   I have often seen the private nurse go on dusting..while the patient is eating... The above remarks apply much more to private nursing than to hospitals.
>
> 1934   P. Bottome *Private Worlds* xii. 114   They stood in a small private room off the ward, and looked down at the moaning woman on the bed.
>
> 1956   P. Scott *Male Child* i. i. 26   I spent most of April in a private nursing home.
>
> 1967   P. Willmott *Consumer's Guide Brit. Social Services* vi. 158   Financial help towards the cost of private treatment is provided by several provident associations.
>
> 1976   N. Leigh-Taylor *Doctors & Law* iv. 35   The Government has announced that it intends..to abolish private treatment in N.H.S. hospitals.
>
> 1996   *Private Eye* 13 Dec. 14/2   Presumably some of the patients who get hacked off waiting 18 months for an appointment decide to go private.

c. Of, designating, or belonging to an industry or business conducted or controlled by an individual or independent (commercial) body, rather than a public body or the State. Frequently in *private company n.*, *private sector n.* at Compounds 2.

> 1641   T. Roe *Speech Parl.* 5   We have yet another great help which is our owne..which is our fishing and erecting of Busses..and this by private industry (though to private losse) is beaten out already.
>
> 1723   F. Hutchinson *Let. Member Parl.* 3   Improving the Ground must be carried on by private Industry, and Experiments of ingenious Men, more than by publick Laws.
>
> 1790   J. A. Park *Syst. Law Marine Insurances* (ed. 2) i. 9   Any policy subscribed by a private firm or partnership, is absolutely void.
>
> 1872   S. A. Foot *Autobiogr.* 140   I am not aware that any private corporation in this state can sue or be sued except in its corporate name.
>
> 1934   *Clearfield (*Pa.*) Progress* 5 Oct. 4/1   The government..has had much to say about certain practices in the private business world by which fictitious values were created and traded on.
>
> 1978   W. W. Rostow *Getting from Here to There* xiii. 227   Growth was driven forward by..the expansion of public and private services facilitated by rapidly rising real incomes.
>
> 2005   *Western Daily Press (*Bristol*)* (Nexis) 21 Dec. 32   He has secured around £5million in private backing for his electro-kinetic road ramp which is set to go into production next year.

3.

a. Concerning, involving, or affecting a particular person or group of people apart from the general community; individual or personal, rather than communal or shared.

a1400   *Clensyng Mannes Sowle* in *Eng. Misc. presented to Dr. Furnivall* (1901) 264   Priuate penaunce is that penaunce which is done alday whan a man will priuely be confessed of his schrift fadir.

c1475   (‣ c1445)   R. Pecock *Donet* (1921) 131 (*MED*)   Neiþir bi story which þe disciplis and heerers of þe apostlis han writen, neiþir bi surest priuate reuelacioun, it is open þat crist maad enye suche positive lawe.

1526   W. Bonde *Pylgrimage of Perfection* II. sig. Ki   Onely for their priuat profyte.

1560   J. Daus tr. J. Sleidane *Commentaries* f. xxxiiijᵛ   Certen priuate dyspleasures did growe betwixte hym and the Frenche kynge.

a1616   W. Shakespeare *Julius Caesar* (1623) II. ii. 73   For your priuate satisfaction..I will let you know.

1651   T. Hobbes *Leviathan* II. xxii. 122   He, whose private interest is to be debated.

1776   A. Smith *Inq. Wealth of Nations* I. I. x. 177   When masters combine together in order to reduce the wages of their workmen, they commonly enter into a private bond or agreement.

1838   C. Thirlwall *Hist. Greece* (new ed.) II. xv. 260   In reality they had only consulted their own private ambition.

1883   *Law Rep.: Queen's Bench Div.* **11** 597   That the censure had been made injuriously and from motives of private malice.

1949   *Archit. Rev.* **105** 248   The days when the designer ignored everything that didn't fall into line with his own private taste.

1992   *N.Y. Times Mag.* 31 May 44/3   Fingers splayed in private ecstasy, [he] starts dancing all over the stage.

†**b.** Peculiar to a particular person, community, etc.; particular or special. *Obsolete.*

1526   *Bible (*Tyndale*)* 2 Pet. i. 20   So that ye fyrst knowe this, that no prophesy in the scripture hath eny private interpretacion [Wyclif ech prophecie..is not maad bi propre interpretacioun; Coverdale no prophecie..is done of eny priuate interpretacion; *Geneva* is of any priuate motion; *Rhem.* is made by priuate interpretation; 1611 is of any priuate interpretation.]

1559   in J. Strype *Ann. Reformation* (1709) I. App. viii. 20   The realm of Englande hath been alwaies governyd by private lawes and customes.

1593   T. Bilson *Perpetual Govt. Christes Church* vii. 86   Neither was this priuate to Timothie, but..it was vsuall in the Apostles times.

1651   C. Cartwright *Certamen Religiosum* I. 120   How can any man assume to himselfe a freedome from Erring by the assistance of a private Spirit?

 c. *Biology*. Of a protein, mutation, etc.: occurring only in a restricted population.

1956   *Science* 13 Apr. 633/2   It would seem that the Diego factor is not a 'private' blood group, but rather that its incidence is high in Indians.

1969   *Vox Sanguinis* **17** 305   The new private antigen Ptᵃ is probably inherited as a Mendelian dominant.

1991   *New Scientist* 7 Dec. 31/2   Some mutations, so-called 'private' mutations, are so rare that they occur in only one family.

2004   *Diabetes Care* (Nexis) **27** 1798   In Ojibwa-Cree indigenous Canadians, a private mutation..present

in 20% of the population predisposes to diabetes.

4.

a. Of or relating to a person as an individual or in a non-official capacity; not connected with one's work or official position. Frequently in *private life n.* at Compounds 2.

> 1421   in W. Fraser *Douglas Bk.* (1885) III. 242   Archibald erle of Douglas..Giffin onder owr prewait seill.
>
> a1525   *Bk. Chess* l. 762 in W. A. Craigie *Asloan MS* (1923) I. 105   Thir Iudges suld richt veill attend fra pryvate luif.
>
> 1613   S. Purchas *Pilgrimage* 286   In a priuate habit he visited the Markets, and hanged vp the hoorders of coine.
>
> a1668   W. Davenant *Play-house to be Let* iv, in *Wks.* (1673) 109   Kings who move within a lowly sphear of private love, Are too domestick for a Throne.
>
> 1713   R. Steele in *Guardian* 30 May 1/2   The private Letters of great Men are the best Pictures of their Souls.
>
> 1797   W. Godwin *Enquirer* I. vii. 59   A private pupil is too much of a man.
>
> 1830   *Chron.* in *Ann. Reg.* 259/1   The eldest of three sons of the grand-duke Charles-Frederick, by his *morganique*, or private-marriage, with Louisa-Caroline, countess of Hochberg.
>
> 1878   W. E. H. Lecky *Hist. Eng. 18th Cent.* I. i. 161   The influence which his good private character..once gave him had been rapidly waning.
>
> 1885   *Atchison (*Kansas*) Daily Globe* 1 May   A communication..by the State Veterinary Surgeon... 'I went to Fulton as a private investigator nearly three weeks ago.'
>
> 1920   H. Begbie *Mirrors of Downing St.* 7   The private opposition he [*sc.* Lloyd George] encountered in Downing Street.
>
> 2002   D. D. N. Nsereko *Constit. Law in Botswana* ii. ii. 82   An interesting issue that is not directly addressed by the Constitution is whether the President can consent to being sued in his private capacity.

b. Of a person or company of people: not holding public office or official position; not officially recognized or authorized.

> 1437   *Rolls of Parl.* IV. 508/1   The commen sale and issue of alle ye Wolles..have been..hindred..by specialle licences graunted to private personnes, a part for to selle hir owne Wolles and Wollefelles at large for his singuler avauntage and ayeinst ye commen prouffit.
>
> ‣ a1475   J. Fortescue *Governance of Eng.* (Laud) (1885) 125   He lyved..in more subgeccion than doth a priuate person.
>
> 1549   *Bk. Common Prayer* (STC 16267) Ceremonies f. xxxv*   The appoyntmente..pertayneth not to pryuate menne.
>
> 1589   G. Puttenham *Arte Eng. Poesie* I. xxiv. 38   It [*sc.* war] toucheth the whole state, and euery priuate man hath his portion in the damage.
>
> 1644   J. Milton *Areopagitica* 16   No Poet should so much as read to any privat man, what he had writt'n.
>
> 1673   J. Ray *Observ. Journey Low-countries* 305   When the Gallies are at home those [slaves] that belong to private persons are permitted to lodge in their Masters houses.
>
> 1712   R. Steele *Spectator* No. 429. ⁋8   A Woman of Quality; married to a private Gentleman.

1776   A. SMITH *Inq. Wealth of Nations* I. I. ix. 113   As the capital of a private man..may increase beyond what he can employ in it..so may likewise the capital of a great nation.

1817   J. EVANS *Excursion to Windsor* 72   It was a most uncommon thing for a private man, and a commoner, to be honoured with so long an audience.

1885   *List of Subscribers Exchange Syst.* (United Telephone Co.) (ed. 6) 233 (*advt.*)   The Birkbeck Bank opens Drawing Accounts with trading firms and private individuals.

1930   G. B. SHAW *Apple Cart* p. xix   We cannot do this as private persons. It must be done by the Government or not at all.

1993   *Time Internat.* 18 Jan. 30/3   Godwin's group is advocating that the government let private individuals use the most powerful encryption systems.

†**c.** Of a city or town: not forming a seat of government; not a capital. *Obsolete. rare.*

1632   W. LITHGOW *Totall Disc. Trav.* VII. 334   This Citty..was once the Capitall seat of the Kingdom, though now..it is onely become a priuate place.

5.

a. Belonging to or forming the exclusive property of a particular individual, company, etc.

1442   in A. H. Thompson *Visitations Relig. Houses Diocese Lincoln* (1919) II. 52   Ye and thai aftere your rewle lyfe in commune..levyng vtterly all pryuate hydles, chaumbres and syngulere housholdes.

*c*1484   (‣ *a*1475)   J. DE CARITATE tr. *Secreta Secret.* (Takamiya) (1977) 135 (*MED*)   It is conuenient..to haue in hys howsold priuat seruauntys.

?1504   W. ATKINSON tr. Thomas à Kempis *Ful Treat. Imytacyon Cryste* (Pynson) III. 221   The xxxi. chapiter, the loue of pryuate thynges & of mannys selfe letteth the perfyte goodnes of mannys soule.

1560   J. DAUS tr. J. Sleidane *Commentaries* f. cxxvij   They teache howe it is not lawful for the christians..to haue any thynge priuate, y^t al things ought to be common.

1598   E. FORD *Parismus* xxi. sig. X   Shee went out of the Prison, by a priuate Key which shee had alwayes about her.

*a*1616   W. SHAKESPEARE *Julius Caesar* (1623) III. ii. 241   He hath left you all his Walkes, His priuate Arbors,..On this side Tyber.

1638   F. JUNIUS *Painting of Ancients* 147   As for private Libraries, Martial teacheth us, That in them the Images of such Writers as were as yet surviving, might bee admitted.

1690   J. LOCKE *Ess. Humane Understanding* III. xi. 254   For Words..being no Man's private possession, but the common measure of Commerce and Communication.

1799   W. TOOKE *View Russ. Empire* II. 531   The late empress having..relinquished her imperialties on the private mines.

1840   C. THIRLWALL *Hist. Greece* VII. 335   He sent back his brother Menelaus..together with his private baggage.

1899   *Westm. Gaz.* 21 Sept. 4/1   He hoped it would not go forth from the Conference that they wanted to stamp out all private venture schools.

1942   *Antiquity* **16** 96   The establishment was certainly built as a private burial-place by a prominent local family.

1991   R. Ferguson *Henry Miller* vi. 106   He had a large estate in Scarsdale and a private golf course.

b. Of a ship: *(a)* privately owned, operating commercially; see also *private man of war n.*, *private ship of war n.* at Compounds 2; *(b)* (in the Royal Navy) under the command of a captain only, rather than a commodore or admiral.

1610   P. Holland tr. W. Camden *Brit.* 36   What with ships for convoy of corne and victuals, and what with other private vessels that every man had built for to serve his owne turne, there was 800. saile and above.

1636   *Welwood's Abridgem. Sea-lawes* (new ed.) xxviii. 240   Captaines of Princes warfare-shippes should be..vigilant, diligent, and carefull... Their commandement and power over their company, not onely surpasseth the power of Masters and Commanders of private shippes, but also that of the Captaines on land.

1708   T. Langham *Neat Duties on All Merchandize* 176/1   Imposition... Cloth on Private Ships, *20 per Cent.*

1790   *Aberdeen Mag.* 23 Sept. 565/1   It was the intention of the Minister that he should embark in a private vessel, without Government appearing to have any concern in it.

1845   *Jrnl. Royal Geogr. Soc.* **15** 294   Letters are made up by a local post-office, and sent to Lisbon by private ships.

1909   *Times* 25 May 14/4   The *Boadicea* is to commission first as a private ship, but will subsequently relieve the *Topaze*, flying the broad pennant of commodore.

1986   N. A. M. Rodger *Wooden World* (1988) i. 18   The decisions of a young commander of a sloop cruising alone might be more difficult than those of a senior post-captain commanding a private ship in a large squadron.

2005   *Malaysia Gen. News* (Nexis) 4 Jan.   Donations..had been collected for tsunami victims in Acheh and would be sent via Port Klang tomorrow with the help of the Malaysian Navy and private vessels.

6. Kept or removed from public view or knowledge; secret; †concealed (*obsolete*).

1472–3   *Rolls of Parl.* VI. 29/2   After that dyvers of the Lordes and Knyghtes of the Shires were departed, by mervelous pryvat labour a Bille signed by the Kyng was brought to the seid Commens.

1533   J. Bellenden tr. Livy *Hist. Rome* (1901) I. 225/12   The faderis, movit to hie displeseris be thir persand wourdis, held..mony private consultatiouns.

1594   W. Shakespeare *Henry VI, Pt. 2* ii. ii. 60   In this priuate place, be we the first to honor him with birthright to the Crown.

1615   R. Brathwait *Strappado* 120   Which he suspecting, lay in priuate wait, To catch the knaue.

1669   R. Mountagu in *Buccleuch MSS* (Hist. MSS Comm.) (1899) I. 441   She desired..to send it over in my name, because that way it would be privater.

1700   J. Tyrrell *Gen. Hist. Eng.* II. 842   He lay private, till his Peace was made with the King.

1726   G. Leoni tr. L. B. Alberti *Architecture* I. 52/1   If the sound comes to you dead, and flat, it is a sign of some private [It. *interna*] infirmity.

1753   S. Richardson *Hist. Sir Charles Grandison* VI. xliv. 280   No hugger mugger doings—Let private weddings be for doubtful happiness.

1839   C. Dickens *Nicholas Nickleby* lx. 594   The same love of gain which led him to contract this marriage, led to its being kept strictly private.

1890   *Lippincott's Monthly Mag.* Jan. 13   It should be kept private for a time.

1977   *Audubon* May 4   The nest site is kept hidden, the jays approach it secretly, and nest-building and egg-brooding are very private.

1991   H. Brodkey *Runaway Soul* 360   One's illicit uncensored private responses to war stuff was maybe a wistful and vicarious viciousness or a heroic unvicarious viciousness.

7.

a. Of a conversation, communication, etc.: intended only for or confined to the person or persons directly concerned; confidential.

1560   J. Daus tr. J. Sleidane *Commentaries* f. cxiij^v   The byshoppes hauynge priuate talke with the Quene.

1650   W. Brough *Sacred Princ.* 285   Private Confession is reteined in the Reformed Churches.

1734   Bp. J. Stearne *Let.* 25 June in J. Swift *Corr.* (1965) IV. 236   I shall put off my defence till I have the pleasure of half an hour's private conversation with you.

1791   A. Radcliffe *Romance of Forest* I. vi. 222   I supplicate of you a few moments private discourse.

1857   A. Trollope *Barchester Towers* xlvii   He received a letter, in an official cover, marked 'private'.

1894   'A. Hope' *Prisoner of Zenda* ix. 128   I could hear no words, but Detchard's head was close to that of the taller of his companions... 'H'm! Private communications,' thought I.

1940   R. S. Lambert *Ariel & all his Quality* ix. 244   A letter was delivered..addressed 'H. Brown, Esq., Broadcasting House'. It was not marked 'Personal' or 'Private'.

1991   *N.Y. Times Mag.* 1 Dec. 30/2   Most of us miss these allusions; they are private communications to the cognoscenti.

†**b.** Of a person: intimate or confidential (*with* a person); sexually intimate. *Obsolete.*

1574   E. Hellowes tr. A. de Guevara *Familiar Epist.* 274   The Court is not but for men y^t be priuate and in fauour, that can gather the frute thereof.

1612   J. Webster *White Divel* III. i. 20   My lord duke & she have been very private.

1641   W. Mountagu in *Buccleuch MSS* (Hist. MSS Comm.) (1899) I. 286   The King is often very private with Digby and Bristow.

1648   T. Gage *Eng.-Amer.* 205   A great Politician, and very familiar, private, and secret with the Archbishop of Canterbury.

1821   Ld. Byron *Marino Faliero* (2nd issue) IV. i. 102   Dismiss This menial hence; I would be private with you.

8. *Telephony* and *Telegraphy*.

a. Of a telephone or line: that is permanently for the exclusive use of the subscriber, or not connected to the public network. Of a number: *(a)* ex-directory; *(b)* belonging to a private address rather than business premises. Chiefly in *private line n.*, *private number n.* at Compounds 2.

1852   L. Turnbull *Lect. on Electro-magnetic Telegr.* 137   Nearly all the railroad companies have private

lines for their own use, and preparations are now making, which..will include every town..throughout Germany in this network of communications.

1878   *Telegr. Jrnl.* **6** 51/1   The regulations concerning the despatch and receipt of telegrams, the tariffs for the same, and for the renting of private wires.

1924   J. Buchan *Three Hostages* xvi. 235   This must be a private telephone..of which only his special friends knew the number.

1976   T. H. Flowers *Introd. Exchange Syst.* i. 11   Picture telegraphy..is possible over the telephone service lines but difficulties discourage small users and encourage large users of such services to rent private circuits not subject to switching.

1990   J. Bradshaw *Homecoming* x. 203   I changed my private phone number..to an unlisted number.

1996   *Vancouver Sun* 13 Apr. A17 (*advt.*)   Service will not provide numbers from cellular callers or call blocked or private numbers.

 b. Designating components of an exchange circuit whose electric potential indicates the condition of a particular subscriber's line, used to test whether the line is in use without interfering with a call in progress. Frequently in *private wire n.* at Compounds 2.

1852   *Times* 20 July 3/6   The merchants and stockbrokers of this country..will form their own opinions as to the propriety of A K messages and private wires.

1906   J. Poole *Pract. Telephone Handbk.* (ed. 3) xxx. 486   When a current is started and stopped through the 'private' magnet, the end of the side-switch arm slips under the outer tooth.

1919   R. Mordin *Strowger Automatic Telephone Exchange* i. 23   The whole arrangement of fixed contacts is called the connector bank; the upper half the private bank, and the lower the line bank.

1942   J. Poole *Telephone Handbk.* x. 238   The potential on the private conductor throughout the call is normally that of earth.

1969   S. F. Smith *Telephony & Telegr. A* vi. 153   A third wire is therefore provided on all connexions through the exchange, the potential of which indicates the condition of the circuit. This avoids intrusion on calls in progress and is called the private wire, usually abbreviated to 'P-wire'.

 c. Of a telephone exchange: serving private lines. Chiefly in *private branch exchange n.* at Compounds 2.

1891   J. Poole *Pract. Telephone Handbk.* vii. 124   Fig. 102 represents a type of switch-board which was designed by the writer in 1881 for the use of private telephone exchanges.

1983   *New Scientist* (BNC) 28 Apr.   Mercury is waiting for Telecom to connect its equipment with a private telephone exchange.

1998   *What Cellphone* Aug. 104/3 (Gloss.)   *PABX* , Private Automated Branch Exchange. Automated multi-extension exchanges or switchboards as used nowadays by most offices.

 II. Relating to or connected with activities restricted to one person or a few people.

 9. Of a place: unfrequented, secluded; affording privacy.

*a*1513   R. Fabyan *New Cronycles Eng. & Fraunce* (1516) I. clix. f. lxxxviiᵛ   Yᵉ sayd Bysshoppes were depryued of theyr dignyties and put into pryuate Houses of Relygyon.

1662   J. RAY *Three Itin.* II. 162   We went to Shap,..where we saw the ruins of the abbey, very pleasantly situate in a private valley.

1746   P. FRANCIS & W. DUNKIN tr. Horace *Satires* I. ix. 145   In private haunt, in public meet, Salute, escort him through the Street.

1750   *Bible (*Challoner*)* III. Psalms x. 8   He sitteth in ambush with the rich in private places, that he may kill the innocent.

1756   J. WOOLMAN *Jrnl.* (1971) i. 29   I frequently withdrew into private places and often with tears besought the Lord to help me.

1817   J. EVANS *Excursion to Windsor* 192   I scarce go out of my own house, and then only to two or three very private places, where I see nobody that really knows anything.

1896   A. R. WHITE *Youth's Educator* iv. 36   She reserves all those disagreeable fashions for a more private place.

1924   *Nevada State Jrnl.* 6 Dec. 1/1   The train on which Mr. Coolidge returned was more private.

1991   J. PHILLIPS *You'll never eat Lunch in this Town Again* (1992) 345   The first thing one needs to find is a private place for bathroom requirements.

10. Of a person, etc.: retiring, reclusive; living a quiet or secluded life; reserved, unsociable.

1585   R. PARSONS *Christian Directorie* II. i. 191   S. Antony..a little before had professed a priuate and a solitarie life in Egypt.

1599   M. DRAYTON *Idea* in *Englands Heroicall Epist.* (new ed.) sig. P5   O God from you that I could priuate be.

1630   tr. G. Botero *Relations Famous Kingdomes World* (rev. ed.) 58   Their women are very private, fearefull to offend.

1673   R. LEIGH *Transproser Rehears'd* 79   How one of his private condition and breeding could arrive to this degree of court-ship.

1759   R. JACKSON *Hist. Rev. Pennsylvania* 379   'Tis true, but..so very private, that in the Herd of Gentry they are hardly to be found.

1850   L. HUNT *Autobiogr.* xvii. 267   The privatest of all public men found himself complimented.

1991   *Vanity Fair (*N.Y.*)* Sept. 240/2   Unlike the Bloomsburys,..the leading writers in London today tend like Drabble and Holroyd to be very private.

11. Of a person or two people: alone; undisturbed by others.

1599   W. SHAKESPEARE *Romeo & Juliet* I. i. 134   Away from light steales home my heauie sonne, And priuate in his Chamber pennes himselfe.

1623   W. SHAKESPEARE & J. FLETCHER *Henry VIII* II. ii. 14   I left him priuate, Full of sad thoughts and troubles.

1752   S. FOOTE *Taste* I. 3   Let us be private.

1851   H. MELVILLE *Moby-Dick* iii. 17   No man prefers to sleep two in a bed... I don't know how it is, but people like to be private when they are sleeping.

1928   D. H. LAWRENCE *Lady Chatterley's Lover* x. 140   A man could no longer be private and withdrawn. The world allows no hermits.

1983   J. LINGARD *Winter Visitor* i. 9   Ed Black wanted to be private, you could tell that at a glance.

†**12.** Privy *to*; = PRIVY *adj.* 4a. Also with *with*. *Obsolete*.

> 1601   B. JONSON *Fountaine of Selfe-love* I. ii. sig. B3ᵛ   Had Eccho but beene priuate with thy
> thoughtes.

> ?1635   F. QUARLES *Argalus & Parthenia* (new ed.) II. 81   Not making any private to her flight, She quits the
> house, and steales away by night.

> 1742   *Cervantes' Novels, Lady C. Bentivoglio* 92   That Maid-servant of mine, who was private [1640 privie]
> to my Actions.

†**13.** Of a person: secretive, reticent; discreet, dependable in confidential
matters. *Obsolete*.

> a1625   J. FLETCHER *Wife for Moneth* I. i, in F. Beaumont & J. Fletcher *Comedies & Trag.* (1647) sig.
> Ffffff4ᵛ/1   You know I am private as your secret wishes, Ready to fling my soule upon your service.

> 1660   A. MARVELL *Let.* 8 Dec. in *Poems & Lett.* (1971) II. 9   We hope you will be private in these things
> communicated to you out of faithfulness to your intrest.

> 1824   W. SCOTT *Redgauntlet* II. xii. 278   You must give me yours [*i.e.* your word] to be private in the
> matter.

B. *adv.*

Privately; secretly, in private. Now chiefly *regional* and *nonstandard*.

> ‣ c1443   R. PECOCK *Reule of Crysten Religioun* (1927) 364   Alle þe lyuyng of religiose persoones which þei
> leeden priuate and singuler..comeþ into þe lawe of god.

> a1592   R. GREENE *Hist. Orlando Furioso* (1594) sig. Hiiᵛ   Nere had my Lord falne into these extreames,
> Which we will parle priuate to our selues.

> 1660   S. PEPYS *Diary* 6 Mar. (1970) I. 79   Everybody now drink the King's health..whereas before it was
> very private that a man dare do it.

> 1704   J. TRAPP *Abra-Mule* I. i. 117   I came private, and unattended.

> 1759   J. SHUTER *Let.* 1 July in *Beekman Mercantile Papers* (1956) II. 663   The busnes Was Careyed on So
> privet that I did not know of it until it was all over.

> 1821   W. SCOTT *Kenilworth* I. viii. 202   He..came not thither so private but what he was espied by one who
> told me.

> 1876   'M. TWAIN' *Adventures Tom Sawyer* xxxv. 272   I'll smoke private and cuss private.

> 1905   A. M. BINSTEAD *Mop Fair* viii. 135   They arranges to stop 'private' in Brighton, at a little case in Black
> Lion Street where Tom Reeder annually took his old woman every August.

> 1977   I. SHAW *Beggarman, Thief* I. ii. 25   We got some things to talk about together, private, him and me.

> 1996   C. I. MACAFEE *Conc. Ulster Dict.* 262/2   *Private*, privately, thus live private live on a private income.

C. *n.*
I. A private affair or thing.
1.

a. *in private*: privately, confidentially, or secretly; in private company;
in private life. Formerly also †*on private*.

1469   *Charter Edinb. Reg. House* No. 419   I sall neuer in privat nothr in part be me or ony otheris..hendyr [etc.].

1581   R. MULCASTER *Positions* xxxix. 188   Doth not that deserue to be liked on in priuate, which is thoroughly tryed being showed forth in common?

1582   R. STANYHURST tr. Virgil *First Foure Bookes Æneis* I. 9   Hee walcks on priuat with noane but faythful Achates.

1615   G. SANDYS *Relation of Journey* 171   Confesse they do, but not greatly in priuate.

1672   R. BAXTER *Church told of Bagshaw's Scandals* iii. 32   Could you wish..that the..Protestant Religion were kept up by none but the unconformable Ministers in private?

1732   T. LEDIARD tr. J. Terrasson *Life Sethos* II. IX. 273   You are absolutely forbidden speaking to him in private.

1791   A. RADCLIFFE *Romance of Forest* I. v. 197   If you must be tyrannical, Madam, indulge your humour in private.

1832   H. MARTINEAU *Life in Wilds* vi   Let each family eat in private.

1896   C. G. D. ROBERTS *Forge in Forest* viii. 101   Would you speak with me in private, Father?

1952   B. DAVIDSON *Rep. S. Afr.* I. i. 27   No serious South African will argue any longer (at least in private) that *apartheid*..can work.

1992   *Face* Feb. 14/2   Ashley..[is] willing to say in print what many more are muttering in private.

†**b.** Seclusion, privacy. *Obsolete.*

*a*1616   W. SHAKESPEARE *Twelfth Night* (1623) III. iv. 88   Go off, I discard you: let me enioy my priuate .

*a*1641   J. WEBSTER & T. HEYWOOD *Appius & Virginia* (1654) II. 11   I see there's nothing in such private done, but you must inquire after.

*a*1657   G. DANIEL *Idyllia* in *Poems* (1878) IV. i. 58   Perhaps I have To my owne Private, had reflects, as grave On my Condition.

†**2.**

 a. A private or personal matter, business, or interest; (in *plural*) private affairs. *Obsolete.*

1549   N. RIDLEY *Let.* in R. Potts *Liber Cantabr.* (1855) I. 245   [Letters] to signifye..the priuits of my hart and consciance.

1592   H. UNTON *Corr.* (1847) 289   I will no longer hold your Lordship with this my privatt.

1606   W. WARNER *Continuance Albions Eng.* XV. xcvi. 383   Phocas for his Priuats Rome the Supreme Sea promoted.

1611   B. JONSON *Catiline* III. sig. G2ᵛ   Nor must I be vnmindfull of my priuate .

1642   J. MARCH *Argument Militia* 7   When it concerns any mans private.

1674   R. JOSSELIN *Diary* 10 May (1976) 575   My private very afflictive.

b. A private opinion. *Obsolete. rare.*

1599   A. DAY *Eng. Secretorie* (rev. ed.) I. sig. U1   Yet may you vouchsafe in your owne priuate to reckon

mee with the greatest in willingnesse.

†**3.** A lavatory; = PRIVY *n.* 1. *Obsolete. rare.*

> 1600   J. HAMILTON *Facile Traictise* Sacram. 281   Ʒoung wemen..casting thair new borne babes in filthie priuets, vthers in colpots, and in vther secret places.

4. In *plural.* The genitals. Cf. *private parts n.* at Compounds 2.

> In quot. 1604   also punningly with sense C. 9a.

> 1604   W. SHAKESPEARE *Hamlet* II. ii. 236   In the middle of her fauours..her priuates we.
>
> 1756   M. MOONEY *Diss. Nature & Cure Venereal Dis.* 12   They both affect the Privates in the same Manner.
>
> 1772   N. D. FALCK *Treat. Venereal Dis.* I. ii. 28   Women have naturally many discharges from their privates, to which men are strangers with theirs.
>
> 1835   A. SMITH *Diary* 29 July (1940) II. 136   They had a piece of skin bound round the body and a piece of rag hanging before the privates.
>
> 1900   G. M. GOULD & W. L. PYLE *Anomalies & Curiosities Med.* xiv. 734   The man..cut off the whole external genital apparatus, remarking as he flung the parts into a corner: 'Any—fool can cut his throat, but it takes a soldier to cut his privates off!'
>
> 1940   C. MCCULLERS *Heart is Lonely Hunter* II. iv. 155   He's so fat he hasn't seen his privates for twenty years.
>
> 1955   S. BECKETT *Molloy* 77   She..thrust her stick between my legs and began to titillate my privates.
>
> 1993   *Sun* 31 May (Summer Soccer Special) 7/2   I kicked the ball across the pitch for a throw-in and it hit my old Cambridge team-mate John Francis in the privates. He dropped like a stone.

†**5.** A private or confidential communication. *Obsolete. rare.*

> a1616   W. SHAKESPEARE *King John* (1623) IV. iii. 16   The Count Meloone,..Whose priuate with me of the Dolphines loue, Is much more generall, then these lines import.

6. *slang.* [Short for *private school n.* at Compounds 2] In the language of British public schools, esp. Eton College: a preparatory school.

> 1925   C. CONNOLLY *Let.* 6 Apr. in *Romantic Friendship* (1975) 64   I met quite a nice small boy who is at my private.
>
> 1932   N. MITFORD *Christmas Pudding* v. 81   At my private..we had a most handy little cemetery for the fathers, just behind the cricket pav.
>
> 1965   *Listener* 22 July 128/1   What private were you at?
>
> 1986   'J. LE CARRÉ' *Perfect Spy* xii. 323   Look here, old boy..I don't think we should go through life wearing hairshirts about what we did at our private.

7. *colloquial.* [Short for *private ward n.* at Compounds 2] = *private ward n.* at Compounds 2.

> 1942   M. DICKENS *One Pair of Feet* vii. 116   People who told me I should be a house-parlourmaid 'on

Privates' had over-estimated. I was Dogsbody.

8. *colloquial.* [Short for *private bar n.* at Compounds 2] = *private bar n.* at Compounds 2.

> 1963   N. Marsh *Dead Water* i. 9   There was only one other woman in the Private beside Jenny.
>
> 1975   A. Hunter *Gently with Love* xxxiii. 132   Come into the private—I would not have you leave without a crack.

II. A private person.
†**9.**

a. A person who does not hold any public office or position. *Obsolete.*

> 1483   *Catholicon Anglicum* (BL Add. 89074) (1881) 291   A Priuate, *priuatus.*
>
> a1616   W. Shakespeare *Henry V* (1623) iv. i. 235   And what haue Kings, that Priuates haue not too, Saue Ceremonie, saue generall Ceremonie?
>
> 1671   J. Milton *Samson Agonistes* 1211   I was no private but a person rais'd With..command from Heav'n To free my Countrey.

b. *the private*: people who hold no public office, as a class. Opposed to *the public. Obsolete.*

> 1716   A. Pope *Corr.* 29 Nov. (1956) I. 377   You have already done enough for the Private, do something for the Publick.
>
> 1744   R. North & M. North *Life Sir D. North & Rev. J. North* 234   Who hath neither Inclination nor Temptation to court the Public, or flatter the Private.

10. An ordinary soldier of the lowest ranks; (in the British Army) a soldier below the rank of lance corporal; = *private soldier n.* at Compounds 2. Also as title. Formerly also: an ordinary sailor of the lowest ranks.

> This rank has many alternative names in different parts of the British Army, as Fusilier, Guardsman, Gunner, Highlander, Kingsman, Rifleman, Sapper, Signaller, Trooper, etc.

> [1756   G. Washington *Let.* 21 July in *Writings* (1931) I. 408   John Coke, who was appointed to your Company, a Sergeant, has since been broke for neglect of Duty. You will receive *him* as *private* and in his room as Sergeant, Mark Hollies.]
>
> 1775   *Jrnl. Continental Congress* **2** 188   Regular companies of Militia..consist of one Captain,..one drummer, one fifer, and about 68 privates.
>
> 1797   *Parl. Reg. 1797–1802* II. 419   The respective increase of monthly pay for able seamen, ordinary seamen, and landmen, with 2d. per day to the non commissioned officers of marines, and 2¼ d. to the privates, would produce a sum total yearly £.351,000.
>
> 1810   Duke of Wellington *Dispatches* (1836) VI. 45   One officer, four serjeants and fifty privates of the 23rd light dragoons.
>
> 1863   *Army & Navy Jrnl. (*U.S.*)* 3 Oct. 84   The privates employed in the Navy are classed in the following

rates.

1898   *Westm. Gaz.* 18 July 5/3   The officerless privates then went in and did nobly.

1918   *Aussie: Austral. Soldiers' Mag.* Aug. 9/2   The C.O. endeavours to persuade Private Hardcase to accept Blighty Leave.

1954   W. FAULKNER *Fable* (1955) 54   Two British privates were resting on the firestep of a frontline trench.

1991   *Combat & Survival* Nov. 12/2   Everyone I spoke to, from the most junior Private to the Commander of 3rd Brigade..seemed confident that they belonged to a team of professionals.

COMPOUNDS

C1.
a. General *attributive* (chiefly in sense A. 2).

private assembly *n.*

1564   A. BACON tr. J. Jewel *Apol. Churche Eng.* sig. Pi   The Bysshops of the weste parte of the worlde didde call togeather Synodes, and make priuate assemblies in their Prouinces.

1621   P. HEYLYN *Microcosmus* 51   These latter being called Hugonotts, so named as they say of a gate in Tours (where they first began) called Hugo's gate, out of which they vsed to goe to their priuate assemblies.

1651   T. HOBBES *Leviathan* II. xix. 99   If it [*sc.* the succession] be in any other particular Man, or private Assembly, it is in a person subject, and may be assumed by the Soveraign at his pleasure.

1797   E. MALONE in J. Reynolds *Wks.* I. p. lv   When not engaged..in some publick or private assembly, or at the theatre.

1842   *Times* 14 Apr. 4/5   He had summoned only a private assembly in a corner of the Reform Club.

1910   *Encycl. Relig. & Ethics* III. 176   The prohibition of public worship drove the people to private assemblies.

1983   *Russ. Rev.* **42** 143   Dostoevsky committed the indiscretions that resulted at once in his arrest, declaiming Belinsky's radical letter to Gogol at more than one private assembly.

2013   C. TAME tr. P. Cossart *From Deliberation to Demonstration* i. 66   If a representative of authority wants to enter a private assembly, the organizer can deny him access.

private baptism *n.*

1549   *Bk. Common Prayer* (STC 16267) Priuate Baptisme f. v*ᵛ, (*heading*)   Of them that be Baptised in priuate houses in tyme of necessitie... Priuate Baptisme.

1662   *Bk. Com. Prayer*   The Ministration of Private Baptism of Children in houses.

1774   *Philos. Trans.* (Royal Soc.) **64** 439   The number of children, who died after receiving only private baptism, in consequence of which their deaths were registered, but not their births, amounts to 17.

1852   J. BEAVEN (*title*)   A manual for the visitation of the sick..to which is added, the office for private baptism.

1996   *Hist. Jrnl.* **39** 1000   The Breslau messenger Merkert, who had baptised his own child, was acquitted by the courts on the grounds that private baptisms were legal.

private boarding house *n.*

1795   *Times* 5 Jan. 4/2 (*advt.*)   Many years established as a private Boarding House.

1818   *Proc. & Rep. Commissioners Univ. Virginia* 21   The dieting of the students should be left to private boarding-houses of their own choice.

1987   *Toronto Star* (Nexis) 14 Jan. A16   If you're troublesome, alcoholic, or restive, chances are you'll be forced by economics to live in places like Channan Court, a notorious private boarding house.

2013   S. ROBINSON *Preventing Emotional Abuse & Neglect* ix. 196   The lack of protections for people living in the private boarding house and hostel sector resulted in many abuses over time.

private brougham *n.*

1848   *Spectator* 5 Feb. 129/2   Hackney cabs would soon get to rival private broughams in their comfort and appearance.

1864   A. TROLLOPE *Can you forgive Her?* I. xxxix. 304   He saw Mrs Greenow issue forth from the Close in a private brougham, accompanied by one of the Fairstairs girls.

1922   J. JOYCE *Ulysses* II. vii. [Aeolus] 143   Hackney cars, cabs, delivery waggons, mailvans, private broughams.

1999   J. GLAVIN *After Dickens* ii. 48   Nicholas himself becomes an idol of the town, rich, feted: ladies of the chorus on every chaise longue, while countesses by the dozen wait near the stage door discreetly expectant in their private broughams.

private carriage *n.*

1787   *Daily Universal Reg.* 17 Jan. 3/2   She was interred in her family-vault at Sutton, in Essex, to which place she was drawn by a hearse and six horses, followed by her own private carriage.

1826   W. HONE *Every-day Bk.* (1827) II. 57   Private carriages..draw up to the box door with a vigorous sweep.

1921   V. WOOLF *String Quartet* in *Monday or Tuesday* 59   Private carriages..have been busy at it, weaving threads from one end of London to the other.

1999   T. MAY *Victorian & Edwardian Horse Cabs* 13   The cabs that they ran were only one type of vehicle amongst many that they made available, others often including omnibuses and hearses or mourning coaches, as well as a variety of private carriages.

private chapel *n.*

1564   T. HARDING *Answere to Iuelles Chalenge* i. f. 25ᵛ   By this decree we learne, that then Masses were commonly sayd in priuat chappelles at home.

1691   A. WOOD *Athenæ Oxonienses* I. 579   He bequeathed all his books, his two Chalices, his Crewetts, holy water stock [etc.]..to his private chappell in London.

1786   *Daily Universal Reg.* 19 Sept. 2/3   Their Majesties attended by four of the Princesses, went to the private Chapel at Windsor, and heard divine service there.

1839   H. W. LONGFELLOW *Hyperion* I. II. ix. 195   Besides, he is known as a man of learning and piety;—has his private chapel, and private clergyman.

1994   *Church Times* 25 Nov. 9/4   Part of the design includes a *tricanale*, which came from the designs of

Andrewes's private chapel.

2009   W. LISTER *Amico* i. 31   The king,..who was known for his piety, heard a simple form of Mass, or devotions, probably early in the morning in the private chapel in the palace.

private communion   *n.*

1564   T. HARDING *Answere to Iuelles Chalenge* ii. f. 42   Many of the places that I alleged in the article before this for priuate communion, may serue to this purpose very wel.

a1649   J. WINTHROP *Hist. New Eng.* (1853) I. 340   Excommunication is no other but when Christians withdraw private communion from one that hath offended.

a1776   D. HUME *Hist. Eng.* (1854–6) IV. xlvii. 443   The rites introduced by James regarded the kneeling at the sacrament, private communion, private baptism, confirmation of children, and the observance of Christmas and other festivals.

1823   M. W. SHELLEY *Valperga* III. 267   We know nothing of the private communion of these friends.

1910   *Encycl. Brit.* I. 974/1   An invalid may always have his private communion.

2003   *Courier Mail (*Queensland*)* (Nexis) 21 June M6   It's the classic image of a little child, wrapped in private communion with a book, oblivious of the clatter from the kitchen, the dog barking, the car accelerating down the road.

private education   *n.*

1581²Priuate education [see sense A. 2b(a)].

1668   D. LLOYD *Memoires* 271   He was..against Fathers keeping their Children at home under their own tuition, because private Education hardly raiseth Youths to that vigor, freedom, and generosity of spirit, that a more publick doth.

1742   S. RICHARDSON *Pamela* IV. liv. 341   He may teach a young Gentleman, betimes, that necessary Presence of Mind, which those who are confin'd to a private Education, sometimes want.

1839   H. T. TUCKERMAN *Isabel* 16   Isabel had reaped the advantages of a faithful private education and occasional visits to the principal cities of her country.

1992   *Economist* 6 June 30/1   Parents opt for private education because they worry that they will have no choice but to send their children to the lousy comprehensive around the corner.

2014   A. PIPER *Educ. in Albuquerque* iv. 37   Several entities chose to open their own schooling system,..and that tradition of private education has continued in the Albuquerque area along side of public schooling.

private funeral   *n.*

1577   R. WILLES & R. EDEN tr. Peter Martyr of Angleria *Hist. Trauayle W. & E. Indies* f. 258ᵛ   Many Bonzii returne lykewise to these priuate funeralles.

1676   E. SETTLE *Conquest of China by Tartars* IV. i. 41   If 'twere by your Sword her Chance to fall, My hand should give her private Funeral.

1766   T. AMORY *Life John Buncle* II. v. 162   I gave her a decent private funeral; a hearse, and one mourning-coach, in which I alone attended her remains to the earth.

1883   *Harper's Mag.* Mar. 648/1   'Well,' said the Pacific sloper, 'if it's a private funeral, what do they call it a reception for?'

2002   *Newsweek* 11 Mar. 42/3   The van Dams plan a private funeral, with a public memorial on March 16 at the beach in La Jolla.

private meeting   *n.*

1576   A. FLEMING tr. Isocrates in *Panoplie Epist.* 175   To thinke of them, as of things in priuate meetings of friends & familiar companions, very requisite & auailable.

1612   W. STRACHEY *Lawes* in P. Force *Tracts* (1844) III. II. 39   Hee shall command all disordred people vntimely (sitting vp late in vsuall assemblies, whither in priuat meetings, publike tap-houses, or such like places) vnto their rests.

1748   S. RICHARDSON *Clarissa* IV. xxxiv. 202   No woman ever gave me a private meeting for nothing; my dearest Miss Harlowe excepted.

1896   *Atlantic Monthly* Aug. 274/1   On the eve of her marriage Clorinda has a private meeting in her house with Sir John.

1995   C. SAGAN *Demon-haunted World* vi. 103   I arranged for McDonald to present his best cases in a private meeting with leading physicists and astronomers.

private play   *n.*

1603   W. SHAKESPEARE *Hamlet* II. iii. 340   Yfaith my Lord, noueltie carries it away, For the principall publike audience that Came to them, are turned to priuate playes, And to the humour of children.

1633   W. PRYNNE *Histrio-mastix* I. VI. v. 495   These Statutes (which are principally intended in private Playes and Enterludes, since they condemne and suppresse all publike,) seeme to allow of popular Stage-playes.

1790   F. REYNOLDS *Dramatist* I. 12   Whence arises the pleasure at an Opera, a private Play, or a Speech in Parliament?

1868   P. FITZGERALD *Life David Garrick* I. vi. 158   It was once determined to get up a private play..and the parts were cast in a moment.

1989   *Independent* (Nexis) 27 Jan. 21   The Duchess of Leinster adopted her, and the Duke of Richmond made her supervisor of his private plays.

2014   D. J. JONES *Sexuality & Gothic Magic Lantern* Introd. 17   The Comte de Caylus frequently used magic lanterns in his private plays.

private theatre   *n.*

1633   W. PRYNNE *Histrio-mastix* II. I. 835   Whether the profession of a Playhouse-Poet, or the penning of Playes for publike or private Theaters, be warrantable or lawfull?

1784   W. HAYLEY (*title*)   Plays of three acts written for a private theatre.

1807   E. WEETON *Let*. 18 Nov. (1969) 50   She..was never outshone in elegance of movement at a Ball, out-performed at a private Theatre.

1999   *N.Y. Times* 19 Oct. E3/4   Grounded in jazz, copping its wit from jump blues, the music Ms. Jones made transformed the American musical canon into her private theater and hiding place.

private theatrical   *n.*

1787   J. Powell (*title*)   The narcotic & private theatricals.

1818   J. Keats *Let.* 23 Jan. (1931) I. 96   I began an account of a private theatrical—Well it was of the lowest order, all greasy and oily.

1831   D. E. Williams *Life Sir T. Lawrence* I. 50   Nor did he ever take part in any private theatricals.

1990   *Vanity Fair (*N.Y.*)* Nov. 76/1   Lust was trench warfare for him, a private theatrical for her.

2007   G. Russell in J. Moody & D. O'Quinn *Cambr. Compan. Brit. Theatre, 1730–1830* xiii. 191   Probably the best-known example of a private theatrical in the Georgian period is..the scheme to stage *Lovers' Vows* in Jane Austen's *Mansfield Park* (1814).

b. Forming adjectives in combination with participles, as †***private-humoured***, ***private-looking***, ***private-spirited***, etc.

1602   W. Fulbecke *Pandectes* 58   Secreat meetinges of male-contents, phantasticall, and priuate humored persons.

1655   J. Sergeant *Schism Dis-arm'd* 19   The Doctors private-spirited opinion.

1709   J. Shaw *Lett. to Nobleman* iii. 19   The sloathful private spirited and inglorious Stranger.

1834   J. L. Motley *Let.* 17 Jan. in *Corr.* (1889) I. ii. 33   The palaces in Berlin being all very simple, private-looking houses.

1895   *Spectator* 21 Sept. 368   Unpatriotic and..private-spirited reason.

1925   *Philos. Rev.* **34** 25   Selfish and private-spirited activities, no less than noble and public-spirited activities, obey this law.

1993   *Time Out* 31 Mar. 41/4   Mostly this is exemplary private-minded, public spirited journalism.

2004   *Bath Chron.* (Nexis) 18 May 30   Housed in a long, low, private-looking building of honey-coloured stone, the sanctuary is all that it says it is—a retreat from bustle and stress.

C2.

private account   *n.* a bank account relating to one's personal (as opposed to business) assets; a credit account for personal purchases.

1772   *Edinb. Advertiser* 2 Oct. 210/2   Had James..any conception that you was indebted upon your own private account?

1785   *Daily Universal Reg.* 16 Sept. 3/2   Above 600,000..sterling per annum have been drawn off on private accounts, by the way of China alone.

1854   C. Norton *Eng. Laws for Women in 19th Cent.* 81   Mr Norton..sent his attorney to make extracts at their bank, of all sums entered in my private account.

1987   W. J. Burley *Wycliffe & Scapegoat* (BNC) 66   On the day Mr Riddle disappeared he drew two hundred and ninety pounds from his private account.

2009   B. Kaye *Marriage First Aid Kit* x. 233   When you have your own private account, you don't have to ask permission for money to implement a private choice.

private Act   *n.* a British parliamentary Act affecting only the interests of a particular individual or small group of individuals (as a corporation, local area, etc.); cf. *public act n.* at Public *adj.* and *n.* Compounds 1b.

*a*1638 R. Brownlow *Rep. Diverse Cases: 2nd Pt.* (1651) 325 Coke cheife Justice..did agree that the Arbitrement, the Convaiance, nor the private Act made nothing in the Case, for by these the Commoner cannot be barred of his Common.

1705 *Laws conc. Poor* vi. 78 Being a private Act none can be indicted.

1818 W. Cruise *Digest Laws Eng. Real Prop.* (ed. 2) V. 527 An estate tail, granted by Richard III. to the Derby family..which by a private act of 4 Jac. I. was limited to the heirs male of the family in a different manner from that in which it had been limited by the letters patent.

1991 J. Kingdom *Local Govt. & Politics in Brit.* xiii. 213 Parliament sometimes extended the provisions of a good private Act to cover all areas by passing a public Act.

2005 E. K. Bankas *State Immunity Controv. Internat. Law* iv. 75 If the act is by its nature such as any private person could engage in, as, for instance, a contract or a loan, the act, whatever its purpose, is a private act.

private army *n.* an army not recruited by the State; a mercenary force; also *figurative* and in extended use.

1857 *Times* 18 Nov. 8/2 His own Contingent was still so strong as not to be immediately controlable by his private army.

1933 E. A. Mowrer *Germany puts Clock Back* 94 The Steel Helmet, or Confederation of Front-line Soldiers, the most respectable of the private armies, was founded on Christmas Day, 1918.

1959 M. Gilbert *Blood & Judgement* ix. 95 The police were a private army.

1968 *N.Y. Times* 23 July 41 (*heading*) Norman Mailer enlists his private army to act in film.

1992 *Utne Reader* Jan. 79/1 With the veneer of the Soviet threat torn away, agency actions prove more than ever a thesis shared by numerous former CIA agents—that the national security apparatus is little more than the private army of the *Fortune* 500.

private bank *n.* a bank owned and run by a small group of people (in Britain, the maximum number was traditionally ten, but this was increased under the 1967 Companies Act to twenty), each partner having unlimited liability.

1696 W. Killigrew *Proposal* 15 That a distinct Appartment, in this Office, shall be fitted; where all Merchants, and Others, may lodge their Cash, as in the Public, or Private Banks.

1714 in A. M. Davis *Tracts Currency Mass. Bay* (1902) 115 Which does most of all import them, the Publick or the Private Bank?

1802 M. Edgeworth *Let.* 1 Dec. in *M. Edgeworth in France & Switzerland* (1979) 43 Private banks never issue any notes.

1978 M. Birmingham *Sleep in Ditch* 120 My mother wanted me to be a banker..in one of the small, distinguished private banks.

2000 *Econ. Affairs* **20** 5/3 Even in countries where private banks do not print the currency today, these institutions do create money when they make loans.

private banker *n.* a person who owns and runs a private bank.

1711 P. H. *Impartial View Two Late Parl.* 104 The Private Bankers, who look'd upon the Bank with an

envious Eye from its first Establishment.

1776   A. SMITH *Inq. Wealth of Nations* I. I. ix. 111   Private bankers in London give no interest for the money which is deposited with them.

1884   *Helena (*Montana*) Independent* 29 Apr. 1/4   The secretary had exercised a wise discretion by depositing money with the treasurer rather than with a private banker.

1978   P. NOYES *Who is Simon Warwick?* viii. 104   A house which only a private banker could possibly have described as a cottage.

2014   D. COX *Handbk. Anti-Money Laundering* viii. 115   When the account is in the name of an individual, the private banker must establish whether the client is acting on his/her own behalf.

private banking *n.* the operations of a private bank.

1757   M. POSTLETHWAYT *Great Britain's True Syst.* ix. 211   By the Means of public and private Banking.

1793   *Edinb. Advertiser* 30 July 74/1   On account of its permanency, such an institution is preferable to private banking.

1818   *Times* 9 Apr. 2/3   The Chancellor of the Exchequer replied, that his regulations went solely to the system of private banking.

1836   in W. L. Mackenzie *Life & Times M. Van Buren* (1846) 176   If the fetters are knocked off by the repeal of the Restraining Law, private banking associations may be formed.

1997   *Investors Chron.* 19 Sept. 32/1   Just two decades ago, reference to private banking in London would only really entail such organisations as Coutts & Co and Hoare & Co.

private bar *n.* = *lounge bar n.* at LOUNGE *n.* Compounds 2; (also) a bar which is not open to the public.

1892   A. CONAN DOYLE in *Strand Mag.* Jan. 79/2   Holmes pushed open the door of the private bar, and ordered two glasses of beer from the ruddy-faced, white-aproned landlord.

1910   H. G. WELLS *Hist. Mr. Polly* viii. 259   The policeman..put his head inside the Private Bar, to the horror of every one there.

1972   M. GILBERT *Body of Girl* xii. 107   She was in here..just after we opened. She came into the private bar.

1992   *Evening Standard* 28 Sept. 11/4   The confused housewife with the naff sofa, and the private bar in her garage.

2007   S. WILLIAMS *Sugar Walls* x. 123   Upstairs would be the two VIP rooms..with a private bar and a private dancing room in each one.

private bath *n.* a bath for private use; (now usually) = *private bathroom n.*

1771   T. SMOLLETT *Humphry Clinker* I. 91   To purify myself from all such contamination, I went to the duke of Kingston's private Bath, and there I was almost suffocated for want of free air.

1825   E. WEETON *Jrnl.* 14 June (1969) II. 384   I like to bathe alone, and a private bath is just to my taste.

1906   'O. HENRY' *Four Million* 47   The double front room with private bath.

1995   *Common Ground* Jan. 32 (*advt.*)   Three bedrooms, each with private bath.

private bathroom *n.* a bathroom set aside for private use, *esp.* one attached to a hotel room or guest room.

> 1857 *Chambers's Information for People* (new ed.) I. 474/2   The establishment should possess washing-rooms, single private bath-rooms, a large plunge bath-room, and waiting-rooms for the several classes of bathers.
> 1910 *Bradshaw's Railway Guide* Apr. 1148   Suites of rooms with private Bathrooms.
> 1995 *Sun* 26 Apr. 23/3 (*advt.*)   All apartments have fully equipped kitchenettes, private bathroom and balconies.

private beach *n.* a beach that is privately owned, esp. by a hotel for the use of guests.

> 1859 *N.Y. Times* 26 Mar. 6/4 (*advt.*)   The location is..near a fine private beach for sea bathing, fine roads, delightful drives.
> 1860 *Times* 26 Dec. 11/5   All the comforts of a country home, fine sea air, a private beach, and the services of an efficient resident governess.
> 1961 *Sphere* 6 May 212   A new 1st-class hotel, the Hibiscus, with private beach, opens this summer.
> 1991 *Holiday Which?* Mar. 108/3   There are no private beaches in Goa, but in peak season guards unobtrusively try to keep the peddlars away from the cream pickings.

private bed *n.* *(a)* a hospital bed in which a patient has privacy; *(b)* (in the United Kingdom) a place allocated for private inpatients at a National Health Service hospital.

> 1855 *Times* 24 Sept. 9/1   For private beds 'revolving fans' are used within mosquito curtains.
> 1927 *Science* 4 Nov. 420/2   The new hospital will contain about 415 public beds, seventy-five private beds and an extensive out-patient department.
> 1967 P. WILLMOTT *Consumer's Guide Brit. Social Services* vi. 158   Private beds amount to little over one per cent of the total number of beds in use.
> 1993 A. GOODMAN *Tell them I'm on my Way* (BNC) 232   There were..approximately 4,000 private beds in NHS hospitals out of a total of 400,000 hospital beds throughout the country.

private bill *n.* (in Britain) a legislative bill affecting only the interests of a particular body or individual; cf. *private Act n.*

> 1572 *Orig. Commons Jrnls.* **2** 101   It is ordered by the house to sytte at afternoones, from three of the clock till six, and to proceede but only in private bills.
> 1678 S. BUTLER *Hudibras: Third Pt.* III. ii. 145   Who..Can..Lay Publick Bills aside, for Private, And make 'em one another Drive out.
> 1785 *Daily Universal Reg.* 9 Feb. 34/3   The House of Peers came to a resolution not to receive any reports from the Judges on private Bills.
> 1844 T. E. MAY *Law of Parl.* 302   The functions of Parliament in passing private bills, have always retained the mixed judicial and legislative character of ancient times.
> 1990 *Green Mag.* Apr. 16/1   Fighting Parliamentary Private Bills has added to the problems facing

conservationists.

Private Bill Office *n.* an office in the Houses of Parliament which deals with business relating to private bills.

> 1819   *Times* 26 Mar. 2/5   Leave might be granted them to deposit in the private bill office, a sectional plan of the property through which the rail-road was to run.

> 1850   in J. Irving *Ann. Our Time* 30 Nov. (1872) 315/1   Plans for about 104 new schemes were deposited to-day in the Private Bill Office.

> 1981   *Legislative Stud. Q.* **6** 502   The last of the older offices, the Private Bill Office, which looks after bills for the benefit of particular interests, dates from the first appointment of a Clerk of Private Bills in 1810.

private box *n.* a box in a theatre which may be booked for the exclusive use of a group of people.

> *a*1640   P. Massinger *City-Madam* (1658) ii. sig. E2   The private Box took up at a new Play For me, and my retinue.

> 1787   *Daily Universal Reg.* 10 Aug. 2/1   Wednesday evening their Highnesses the Prince of Wales and Duke of York were in a private box, at the Hay-market Theatre.

> 1897   R. Kipling *Let.* 1 June in C. E. Carrington *Rudyard Kipling* (1955) x. 254   We went to the Lyceum... Irving put a private box at our disposal.

> 2004   *Sunday Tel.* (Nexis) 28 Mar. 9   It is a beautiful 1,500-seat auditorium with ornate plaster ceilings, faded ruby-red carpets, sloping balcony and gilded private boxes above each side of the stage.

private branch exchange *n. Telephony* an exchange on private premises by which private lines may be connected to a public network; abbreviated *PBX*.

> 1904   *N.Y. Electr. Handbk.* (Amer. Inst. Electr. Engineers) 107   There are at the present time in New York over 5,000 of these private branch exchanges, with a total of over 60,000 stations.

> 1911   W. Aitken *Man. Telephone* xxi. 416   No hotel or warehouse of any standing is now considered complete without a private branch exchange connected to the 'Central' by a number of circuits.

> 1992   *Philadelphia Inquirer* 11 Oct. A24/3   The scam targets the multifunction switchboard used by most corporations—the private branch exchange, or PBX.

private business *n. Eton College slang* extra tuition.

> 1868   *Times* 25 June 10/4   Their tutor used to have a class list of his own for what was called private business, where the ordinary studies of the school were made to give way in favour of English essays.

> 1900   J. S. Farmer *Public School Word-bk.* 158   *Private-business*,..extra work with the tutor.

> 1979   D. Newsome *On Edge of Paradise* ii. 87   Half-an-hour's preparation for his Private Business lecture on Napoleon.

> 1995   *Evening Standard* (Nexis) 14 June 22   Two nights a week boys take part in what the school regards as one of the jewels of its intellectual crown—'private business', or tutorials.

private call *n.* a personal telephone call to or from one's place of work.

> 1907   *Times* 2 Nov. 6/5   Is it likely, with the best intentions on the part of the principals, that these various private calls of *employés* and servants get recorded by the subscriber?
>
> 1942   E. Waugh *Put out More Flags* i. 52   There's a ridiculous woman on the line saying is this a private call?
>
> 1993   S. James *Love over Gold* (BNC) 242   He hoped he at least sounded businesslike, as though it were not a private call.

private car *n.* *(a)* chiefly *U.S.*, a privately owned and used railway carriage; (sometimes also) a railway carriage not available for public use; *(b)* a motor car owned and used privately, contrasted with a commercial vehicle.

> 1826   *Times* 6 July 2/2   Several private cars, on which were ladies, were stopped opposite Colonel White's committee-room.
>
> 1832   *Amer. Rail Road Jrnl.* **1** 495/3   Parties of twenty or more persons can be accommodated..with a private car.
>
> 1897   R. Kipling *Captains Courageous* ix. 186   Send 'Constance', private car, here, and arrange for special [train].
>
> 1926   *Brit. Gaz.* 12 May 1/3   There were few private cars on the roads and nearly every vehicle was labelled 'Food only'.
>
> 1990   *Time* 30 Apr. 23/1   Hanoi's narrow tree-lined streets are filled with bicycles and pedicabs, for private cars are a rarity in the city.

private collection *n.* a collection (esp. of works of art) in private possession.

> 1692   A. Wood *Athenæ Oxonienses* II. 594   In the possession of the other is his Cabinet of Greek Medals, as curious as any private collection whatsoever.
>
> 1751   T. Smollett *Peregrine Pickle* II. lxix. 253   No private collection in Europe was equal to that of Sir Hans Sloane, which, exclusive of presents, had cost an hundred thousand pounds.
>
> 1864   A. Trollope *Can you forgive Her?* I. x. 76   The library, which was the largest of the three, was a handsome chamber, and so filled as to make it well known in the University as one of the best private collections in that part of England.
>
> 1979   R. Cox *Auction* i. 24   There were several Memlings in Austrian private collections. Stefan Zweig owned one.
>
> 1995   *Victorian Soc. Ann. 1994* 27   The exhibition made a profound impression on the young Charles Handley-Read, inspiring him to form the most important private collection of Victorian decorative art ever assembled.

private company *n.* a company in private ownership, as opposed to an organization owned or operated by the State; (now *Law*) a registered company prohibited from offering shares and debentures to the public, and usually having restrictions on membership (cf. sense A. 3a).

?1711   *Some Queries relating to Present Dispute Trade to Afr.* 1   Whether the Government cannot maintain
Settlements abraod as well as a Private Company?

1788   T. JEFFERSON *Memorandum* 14 Apr.   At the village of Kaeferthal is a plantation of rhubarb, begun in
1769 by a private company.

1846   *Jrnl. Statist. Soc.* **9** 212   The want of any general municipal authority has caused the relinquishment of
the street lighting into the hands of private companies.

1908   *Act 8 Edward VII* c. 69 §121   For the purposes of this Act the expression 'private company' means a
company which by its articles—(*a*) Restricts the right to transfer its shares; and (*b*) Limits the number
of its members..to fifty; and (*c*) Prohibits any invitation to the public to subscribe for any shares or
debentures of the company.

1928   *Britain's Industr. Future* (Liberal Industr. Inq.) II. vii. 84   The most important existing legal
distinction is between Public Companies..and Private Companies, limited to not more than 50
shareholders.

1948   *Act 11 & 12 Geo. VI* c. 38 §31   If at any time the number of members of a company is reduced, in the
case of a private company, below two,..and it carries on business for more than six months while the
number is so reduced, every person who is a member of the company during the time that it so carries
on business..shall be severally liable for the payment of the whole debts of the company contracted
during that time.

1996   *Independent* 23 Aug. I. 3/1   Growing numbers of agencies from private companies to central and local
government hold ever-increasing amounts of..information about individuals.

private detective *n.* a detective who is engaged privately, as opposed
to a member of an official police or security force.

1857   *Chicago Tribune* 27 June 1/3   Now if, instead of making indirect charges against private
detectives,..the Mayor would employ some effective means to catch the burglars [etc.].

1861   E. D. COOK *Paul Foster's Daughter* ii. 31   A private detective, ready to peer into anybody's cupboards
and gimletise anybody's doors.

1936   A. CHRISTIE *ABC Murders* v. 38   'Then you're not—anything to do with the police, sir?' 'I am a private
detective.'

1995   *Independent* 23 Nov. 12/7   The authority and the insurers said they would continue to use private
detectives to examine claims.

private developer *n.* an individual who or company which develops
land or property for personal profit.

1911   *Nevada State Jrnl.* 11 Aug. 3/7   The coal fields given over to private developers on a lease hold system
as simple as possible.

1934   *Times* 18 June 11/3   Whether public or private developers take the matter in hand, they will have to act
quickly, for negotiations nowadays are speedy.

1972   *Country Life* 25 May 1330/1   Berkshire has given planning permission for some 18,000 houses, of
which private developers build less than 3,000 new houses a year.

1991   *Power* Sept. 5/3   The island nation is trying to do all it can to attract private developers.

private development *n.* land or property development undertaken by a private individual or company; a property, plot of land, etc., developed in this way.

> 1910 *Times* 30 Apr. 9/1   The best picture in England of the effects of a private development grant.
>
> 1924 H. MOSKOWITZ *A. E. Smith* xli. 271   In every spot in this State where by our past policy we have permitted private development, nobody has benefited but the individuals who have been lucky enough to secure the rights.
>
> 1961 *Recreation* Dec. 531/1   Areas should..have room around the edges to protect the values of the area from encroachment by private developments.
>
> 1992 *Navajo Times (*Window Rock, Arizona*)* Oct. 1/3   In his ruling to end the only quarter-century federal ban on public and private development on Indian lands in the country, [etc.].
>
> 2004 *Independent* 15 May 20/1   The project has Britain's first combined head and power (CHP) system in a private development—an on-site power plant which uses waste and solar energy to provide electricity and central heating for the site.

private dick *n. slang* (originally and chiefly *U.S.*) = *private detective n.*

> 1912 A. H. LEWIS *Apaches N.Y.* vi. 128   But w'at wit' th' stores full of private dicks a booster can't do much.
>
> 1946 E. O'NEILL *Iceman Cometh* I. 14   Yuh remember dey used to send down a private dick to give him the rush to a cure, but de lawyer tells Harry nix, de old lady's off of Willie for keeps dis time and he can go to hell.
>
> 1974 'E. MCBAIN' *Mugger* ii. 14   Bert, on the money I make, I can't afford a private dick.
>
> 2002 *Loaded* July 85/1   Exeter-based Carole-Anne Westcott hired a private dick to track down her runaway husband.

private family *n.* a family in its personal capacity, *esp.* one occupying a private home; a family household as distinct from an institution, commercial establishment, etc.

> 1598 R. BARCKLEY *Disc. Felicitie of Man* IV. 305   Vngodlines troubleth the Church, Iniustice the common wealth, Luxuriousnes priuate families.
>
> 1662 DUCHESS OF NEWCASTLE *Religious* v. xxxviii, in *Playes Written* 555   Indeed happiness lives more in Cloysters than in Courts, or Cities, or private families.
>
> 1751 E. HAYWOOD *Hist. Betsy Thoughtless* I. ii. 20   Never did the mistress of a private family indulge herself, and those about her, with such a continual round of publick diversions.
>
> 1849 T. B. MACAULAY *Hist. Eng.* (1871) I. iii. 144   By the Petition of Right, it had been declared unlawful to quarter soldiers on private families.
>
> 1947 A. B. MEERING *Handbk. for Nursery Nurses* 1   The Nursery nurse who prefers the care of individual children..may become a nanny in a private family.
>
> 2004 *Frederick (*Maryland News-Post*)* 25 Jan. D7/1   Several churches, private families, individuals, businesses and service organizations.

private finance initiative *n.* (also with capital initials) *British* a government scheme under which private sector finance is used to supplement public sector investment in public services, first proposed in 1989, with official guidelines being issued by the Treasury in 1992; abbreviated *PFI*.

> 1989 *Hansard Commons* 22 May 423 The Government will keep up the momentum of the private finance initiative.
>
> 2002 *Metro* 20 Sept. (London ed.) 4/4 Gordon Brown..said it would be 'completely unacceptable' to suspend the Private Finance Initiative, arguing it would deny the public the services they needed.

private function *n.* a private party or other social event.

> 1888 *Times* 3 Dec. 9/5 They held a sort of private function.
>
> 1948 *Sunday Gleaner (*Kingston, Jamaica*)* 17 Oct. 9/3 An opportunity may be made to hear him [*sc.* Paul Robeson] at a private function.
>
> 1995 K. Ishiguro *Unconsoled* viii. 98 If no one had encouraged him, I'm sure he'd have been happy to melt into the background, give the odd recital at a private function, nothing more.

private highway *n.* = *private road n.*

> 1724 *Act to inclose Common Fields Sunningwell cum Bayworth* 2 The said Commissioners..shall ascertain and appoint the publick and private Highways and Roads already made, or to be made..under their Hands and Seals.
>
> 1894 *Oakland (*Calif.*) Tribune* 21 Dec. 8/2 He argued, that their erection would convert a public highway into a private highway for the exclusive use of the railway company.
>
> 1950 *Daily Independent Jrnl. (*Calif.*)* 22 July 3/5 [He] made a left turn into a private highway and was sideswiped by the car following.
>
> 2004 R. H. Buckman *Building Knowledge-driven Organization* vi. 85 I do not understand why any company would try to create its own network in today's electronic world, any more than it would try to build a private highway to truck parts from one plant to another.

private hospital *n.* a hospital which treats only private patients, and which is not funded by the State or a public body.

> 1763 J. Bell *Trav. from St. Petersburg* II. 106 The missionaries also send out people to take up such [children] as have been neglected, who are carried to a private hospital, maintained at their charge.
>
> 1827 *Times* 14 June 2/2 As a general system, he..preferred public asylums to private hospitals, for lunatic paupers.
>
> 1903 *Merck's Ann. Rep.* **17** 183 Veronal has been thoroughly tested in a large number of noted public and private hospitals.
>
> 1990 *Hindu (*Madras*)* 16 Jan. 9/6 Maani Madhava Chakyar died at a private hospital in Ottapalam near here on Monday.

private hotel *n.* a residential hotel or boarding house, usually privately owned, which receives guests only by private arrangement.

1796   *Times* 22 June 1/2 (*advt.*)   J. Morris..fitted up the same in the first stile of elegance, as a private hotel for families and gentlemen.

1820   M. EDGEWORTH *Let.* 14 Nov. in *M. Edgeworth in France & Switzerland* (1979) 274   The Duchesse d'Uzès..has the finest private hotel in Paris.

1936   N. COWARD *Fumed Oak* i, in *To-night at 8.30* II. 41   *Mrs. Rockett*: I can always go to a boarding-house or a private hotel. *Doris*: Catch you!

1962   F. J. BULL & C. RICHARDSON *Hotel & Catering Law* (rev. ed.) iii. 37   The private hotel proprietor reserves to himself the right to pick and choose his guests, and does not hold himself out as willing to receive anyone who calls. He makes a separate contract, either written or verbal, with his guests.

1992   M. WARNER *Indigo* (BNC) 130   Madame Davenant kept a clean and respectable and quiet private hotel, which is why it had been chosen for Miranda and why she liked it.

private income *n.* income derived from private sources, as investments, property, inheritance, etc.; unearned income; = *private means n.*

1725   L. ECHARD *Hist. Revol.* II. i. 117   By sparing her private Income as to her self, she became eminent in her Charities.

1788   in *Federalist Papers* xx. 122   His revenue, exclusive of his private income, amounts to 300,000 florins.

1897   *Lime Springs (*Iowa*) Sun* 2 July 3/3   His wife will make him a small allowance from her private income.

1952   M. LASKI *Village* iii. 65   Because she's got a private income no one ever expected her to go out and take a job.

1991   P. BARKER *Regeneration* iv. 31   I've no private income to tide me over.

private inquiry *n.* work undertaken by a private detective; usually *attributive.*

[1850   *Househ. Words* 27 July 410/1   Sergeant Fendall, a light-haired, well-spoken, polite person, is a prodigious hand at pursuing private inquiries of a delicate nature.]

1856   *Illustr. Times* 2 Feb. 70/3   The design was conceived of establishing a *private inquiry office* with a view of 'preventing and detecting crime'.

1874   M. CLARKE *His Nat. Life* III. xxii. 331   I dabbled a little in the Private Inquiry line of business.

1892   R. KIPLING & W. BALESTIER *Naulahka* xvii. 204   See here, young woman, do you run a private inquiry agency?

1922   *Kelly's Directory Liverpool* 1181/3   Ramage & Kelly private inquiry agents.

1987   D. LINDSAY *Haunted Woman* 185   The police were out of the question, and private inquiry agents were not much better.

private international law *n.* the branch of law which deals with cases of private law involving a foreign element (as the fulfilment of contracts, recognition of marriages and other relationships contracted abroad, etc.), especially in determining the extent to which courts of one's own country have jurisdiction over such cases and whether the domestic or foreign law should be applied by the court to resolving the issue.

1834   J. STORY *Comm. Conflict of Laws* i. 9   The jurisprudence, then, arising from the conflict of the laws of different nations, in their actual application to modern commerce and intercourse, is a most interesting and important branch of public law... This branch of public law may be fitly denominated private international law, since it is chiefly seen and felt in its application to the common business of private persons.

1861   R. PHILLIMORE *Comm. Internat. Law* IV. p. iii   This volume is devoted to the consideration of *Jus Gentium—Private International Law*, or *Comity*: that is, strictly speaking, the law which ought to govern the legal relations of individuals not being the subject of the State which administers the law.

1938   G. C. CHESHIRE *Private Internat. Law* (ed. 2) i. 22   The expression 'Private International Law', coined by Story in 1834,..and used on the Continent by Foelix in 1838,..has been adopted by Westlake and Foote and most French authors. The chief criticism directed against its use is its implication that the subject forms a branch of International Law. There is, of course, no affinity between Private and Public International Law. The latter comprises those universally accepted customs which are recognized by States in their public relations with each other; the former consists of rules which the Courts of each territorial jurisdiction follow when a dispute containing some foreign element arises between private persons.

1992   J. M. KELLY *Short Hist. Western Legal Theory* viii. 346   Mancini's theory had no large-scale success: except within the more modest area of private international law.

private investigator *n.* = *private detective n.*
     In early quots. not a fixed collocation.

[1874   W. G. SUMNER *Hist. Amer. Currency* i. 75   The banks were as recalcitrant about giving statistics, either to the Secretary of the Treasury or private investigators, as about any of their other duties.

1885   *Atchison (*Kansas*) Daily Globe* 1 May   A communication..by the State Veterinary Surgeon... 'I went to Fulton as a private investigator nearly three weeks ago.']

1894   *Standard* 28 Dec. 1/2 (*advt.*)   Eugene Harvey.—Private Investigator. Missing friends found, private inquiries, secret watchings.

1909   *Northeastern Reporter* **86** 375   Also Mrs. Eva Herndon, a private investigator for the United States postal authorities, who testified, in substance, that she had a talk with Mrs. Hagenow at her home on January 22, 1907.

1940   R. CHANDLER *Farewell, my Lovely* iii. 21   Philip Marlowe, Private Investigator. One of those guys, huh?

1995   *i-D* Aug. 48/1   McDonalds sent private investigators to London Greenpeace meetings to sniff out individuals to press charges against.

private joke *n.* a joke understood only by a select few.

1789   *Times* 29 Oct. 2/1   The serious business of the piece is too often disgraced, and the 'cunning of the

Scene' destroyed by their unmeaning merriment and private jokes.

1875   *Harper's Mag.* June 105/1   He was not wanting in a fund of wholesome playfulness, and enjoyed his private jokes with each horse, cow, and hen.

1905   Baroness Orczy *Scarlet Pimpernel* ii. 11   The two little kitchen-maids bustled around..giggling over some private jokes of their own, whenever Miss Sally's back was turned for a moment.

1995   N. Hornby *High Fidelity* (1996) iv. 57   I'd want her to write songs at home, and ask me what I thought of them, and maybe include one of our private jokes in the lyrics.

private judgement *n.* personal opinion (esp. in religious matters), as opposed to the acceptance of a statement or doctrine on authority or on the basis of public opinion.

1565   T. Stapleton *Fortresse of Faith* f. 6   He interpreteth it after his owne liking and priuat iudgement.

1656   T. Blount *Acad. Eloquence* (ed. 2) 11   The more learned have avoided this kinde of flourish, lest their writings should savour more of the general humor, then of private judgement.

1718   T. Herne (*title*)   Defense of private judgment.

1841   T. Carlyle *On Heroes* iv. 201   Liberty of private judgment, if we will consider it, must at all times have existed in the world.

1959   P. Devlin *Enforcement of Morals* 9   Are morals always a matter for private judgement?

2002   *Rev. Politics* **64** 692   The great danger comes in turning all religious questions over to the private judgment of individuals.

private-label *adj.* designating a product manufactured or packaged for sale under the name of the retailer rather than that of the manufacturer; cf. *own-label adj.* and *n.* at own *adj.* and *pron.* Compounds 1.

1923   *Daily Courier (*Connellsville, Pa.*)* 19 Jan. 7/5   No third-rate private label goods are sold at our stores.

1961   *Economist* 11 Mar. 984/1   There are the usual 'private-label' teas, flour, butter, and dried cereals, fruit and pulses; besides these, private label jams and biscuits are quite common and several companies market their own canned peas, soups, canned fruit and canned vegetables; there is even a private-label pine essence.

1995   *Guardian* 14 June I. 17/5   Private label goods are sold by retailers as alternatives to branded products.

private law *n.* the branch of law concerning relations and dealings between private individuals; see quot. 1923.

a1638   R. Brownlow *Rep. Diverse Cases: 2nd Pt.* (1651) 325   Walmesley..sayd, that it was in vain to dispute if the statute of 22 *Ed.* 4. was private Law, or if it were repealed.

1702   G. Mackenzie *Parainesis Pacifica* 6   The third Branch, *viz.* that of Privat Law, cannt [*sic*] afford the least obstruction.

1773   J. Erskine *Inst. Law Scotl.* I. I. 9   Public law is that which hath more immediately in view the public weal... Private is that which is chiefly intended for ascertaining the civil rights of individuals. The private law of Scotland is to be the proper subject of this treatise.

1887   *Jrnl. Hellenic Stud.* **8** 127   Thus the difference between the two cases is the whole difference between private law and public, between Torts and Crimes.

1923 W. J. Byrne *Dict. Eng. Law* 519/2 Private or civil law deals with those relations between individuals with which the State is not directly concerned; as in the relations between husband and wife, parent and child,..contracts, torts, trusts, legacies.

1951 W. H. Jennings *Canad. Law Bus. & Personal Use* i. 6 Private law includes law that is concerned with the regulation of relations between private citizens.

1997 D. P. Kommers *Constit. Jurispr. Germany* (ed. 2) viii. 363 Every provision of private law must be compatible with this system of values, and every such provision must be interpreted in its spirit.

private life *n.* a person's domestic or personal life, as distinct from that relating to his or her employment, official position, public image, etc.

?a1475 (▸ ?a1425) tr. R. Higden *Polychron.* (Harl. 2261) (1872) IV. 419 (*MED*) Galba Seruius..reigned after Nero vij monethes; The priuate lyfe [*Trev.* prive lyf; L. *vita privata*] of whom was noble.

1526 R. Whitford tr. *Martiloge* f. cxxxiv He resygned his crowne, & lyued a holy pryuate lyfe.

1660 G. Mackenzie *Aretina* ii. 205 They see the poverty of a private life, but are strangers to its contentment, and contemns its lownesse without weighing its security.

?1790 J. M. Adair *Unanswerable Arguments against Abolition Slave Trade* v. 173 I think planters are much too remiss on this head; owing to their not employing a little attention to the private life and manners of their slaves.

1843 C. Dickens *Martin Chuzzlewit* (1844) xvi. 193 A full account of the Ball..with the Sewer's own particulars of the private lives of all the ladies that was there!

1943 J. B. Priestley *Daylight on Sat.* xxii. 169 Her own private life, now in ruins, insisted upon claiming her attention, and she could not pretend to herself that it was less important than the private lives of all the other women in the factory.

1992 *Independent* 27 Jan. 20/2 A sense of honour and a degree of self-mastery in private life are virtues in public men and women.

private line *n. Telephony* and *Telegraphy* *(a)* a line that is permanently for the exclusive use of the subscriber or that is not connected to a public network; *(b)* = *private wire n.* (b).

1852 Private lines [see sense A. 8a].

1885 *List of Subscribers Exchange Syst.* (United Telephone Co.) (ed. 6) p. vii The Charge for Private Lines is at a fixed annual rental, payable in advance, varying with the situation and the distance apart of the points connected.

1927 C. W. Wilman *Man. Automatic Telephony* vi. 55 This wire is comparable with the test wire in a manual system inasmuch as it indicates whether a particular line is free or busy... It is..known as the private line (because it prevents intrusion on a busy trunk).

1942 A. Christie *Body in Libr.* vi. 59 I had a private line put in connecting my bedroom with my office.

1993 *Macworld* Dec. 189/1 Dial-up routers let users connect LANs over the wide area using switched services instead of costly private lines.

private man *n.* now *historical* = *private soldier n.*

1651 *Mercurius Politicus* No. 53. 848 This Henry..was little less than a Bastard..; he was also a private man;

and not onely so, but an Exile.

1690   J. MACKENZIE *Siege London-derry* 47/2   Serjeants, Corporals, Drummers, and private Men 2d. per diem each, besides bread.

1796   S. PEGGE *Anonymiana* (1809) 164   Application..on behalf of a private man that had deserted from an independent company just as they were embarking for North America.

1844   *Queen's Regulations & Orders Army* 176   All the Officers, Non-commissioned Officers, Drummers, and Private Men, who may be at Home, are to be accounted for.

1974   L. E. IVERS *Brit. Drums on Southern Frontier* vi. 79   There were six companies, each of which included a captain, lieutenant, ensign, four sergeants, four corporals, two drummers, and one hundred private men who enlisted for seven years.

private man of war   *n.* now *historical* = PRIVATEER *n.* 1; cf. *private ship of war n.*

1646   *MS. Orders & Instruct.* (Adm. Libr.) 22   Instruccions and a fiat in the usuall form were this day signed for Capt. Wm. Davies employing of the ship the 3 kings of dover being of 250 tons and 17 guns as a private man of warre in her way of merchandize.

1675   G. CAREW *Severall Considerations offered to Parl.* 7   The Zelanders are a people, that upon all occations, serves for private men of warr against England.

1754   J. LODGE *Peerage of Ireland* I. 391   Kid had a Commission from the Admiralty, as a private Man of War.

1857   *Rep. Commerc. Relations U.S.* (U.S. Dept. of State) IV. 83   There are only three circumstances when a foreign ship can be made French: they are, 1st. When a prize on the enemy by state ships, or private men-of-war [etc.]

1985   *William & Mary Q.* **42** 361   Ideally, the time at sea for each private man-of-war should be determined, but though colonial newspapers reported hundreds of captures, they did not usually state the length of time the cruisers had been on the hunt.

private means   *n.* income or assets derived from private sources; = *private income n.*

1805   *Times* 20 Mar. 2/2   Mr. Fordyce had brought his salary, and other personal private means, to the public account.

1855   W. SARGENT *Braddock's Exped.* 166   To be reminded that such things as a Press of private means for the benefit of the State still existed.

1994   L. GORDON *Charlotte Brontë* (1995) i. 14   Mr Brontë's failures to secure another wife with private means..had practical consequences for his five daughters.

private motoring   *n.* motoring in a privately owned vehicle.

1916   *Times* 28 June 12/3   It could not be said that the object of the new regulations was either to curtail private motoring or to raise revenue.

1992   B. ELTON *Gridlock* (BNC) 182   When that happens it's going to revolutionize private motoring.

private motorist   *n.* a motorist who drives a privately owned vehicle.

1907   *Times* 8 Aug. 13/2   The private motorist has concluded..that France and Germany would, as hitherto, take the lead in initiating any scientific or technical advance when the progress of the industry required it.

1993   *Computing* 24 June 31/4   It could also be accessed by private motorists via in-car units.

private notice question   *n.* a question put before the House of Commons by prior private arrangement with the Speaker and the person questioned.

[1871   *Hansard Commons* 27 Feb. 941   I wish to ask some questions of the Prime Minister, of which circumstances prevented me from giving any other than a private Notice to him.]

1913   *Hansard Commons* 21 Jan. 225   Private notice question... May I ask the Chancellor of the Exchequer a question of which I have given him private notice.

1964   L. A. ABRAHAM & S. C. HAWTREY *Parl. Dict.* (ed. 2) 168   On specially urgent matters, 'private notice questions' may be asked after the end of the time allotted by the standing orders to questions for oral answer. A member who wishes to avail himself of this privilege must give notice of the terms of his question to the minister and to the Speaker not later than twelve o'clock on the day on which he is to ask it.

2001   R. HOLT *Second amongst Equals* (2002) iii. 88   On his first day in the new job and with a hostile private notice question to deal with (from Michael Foot), Jenkins insouciantly took himself off on a lunchtime engagement.

private nuisance   *n. Law* an unlawful interference with an individual's use or enjoyment of land or rights over land; (also) the offence arising from such an interference; cf. *public nuisance n.* at PUBLIC *adj.* and *n.* Compounds 1b.

1657   W. STYLE *Regestum Practicale* 207   An Action upon the Case ought to be brought against one that makes a private Nusance.

1799   *True Briton* 7 Feb.   If those Gentlemen..thought fit to proceed to indict for a private nuisance, the Defendant was ready to meet them.

1865   *Amer. Law Reg.* **3** 380   Courts of equity will exercise a concurrent jurisdiction with courts of law in cases of private nuisance.

1956   *Country Life* 26 Apr. 866/1   Excessive and disagreeable noise may constitute a private nuisance.

2013   M. WILDE in P. Bishop & M. Stallworthy *Environmental Law & Policy Wales* iii. 32   Lord Jersey was moved to commence an action in private nuisance.

private number   *n. Telephony* *(a)* a number that is ex-directory; *(b)* a number at a private address rather than business premises.

1913   *Times* 28 Nov. 6/1   From my office the operator was instructed to call my private number in the West-end.

1933   D. L. SAYERS *Murder must Advertise* viii. 129   He was not in the telephone-book, but his private number would doubtless be on the telephone-clerk's desk.

1969   N. FREELING *Tsing-Boum* xiii. 95   Good morning. Police Judiciaire!.. I'm at a private number in

> Marseilles; will you..clear me a direct line.

1992   J. MANSELL *Forgotten Fire* (BNC)   She would ring Julius at home, with messages that were only just important enough for her to justify ringing his private number.

private parts *n.* the genitals; also in extended use.

1623   G. MARKHAM *Country Contentm.* i. 35 (*margin*)   The diseases of the priuate parts.

1723   *Oncenia* (ed. 8) 159   Tying a string about my neck, and the other end to my private parts.

1785   F. GROSE *Classical Dict. Vulgar Tongue* at *Commodity*   A woman's commodity; the private parts of a modest woman, and the public parts of a prostitute.

1888   P. H. PYE-SMITH *Fagge's Princ. & Pract. Med.* (ed. 2) I. 188   She mentioned..that she had severe pain in micturition, and that her private parts were swollen.

*a*1930   D. H. LAWRENCE *Last Poems* (1932) 157   The reddened limbs..and the half-hidden private parts.

1971   *Farmer & Stockbreeder* 23 Feb. 30/1   Major Ogilvie recalls some mothers feeling embarrassed at having to see the 'private parts' of an animal's body—like teats and udders—being handled by a man.

1992   S. ARMITAGE *Kid* 70   And his shoulder-blades were two butchers at the meat-cleaving competition and his belly-button was the Falkland Islands and his private parts were the Bermuda triangle and his backside was a priest hole.

private patient *n.* a patient who pays for treatment rather than receiving it free or under subsidy from the State or a public body.

1754Private patient [see sense A. 2b(b)].

1801   *Med. & Physical Jrnl.* **5** 7   Those to whom I have communicated the infection out of the Hospital, or among my private patients.

1859   F. NIGHTINGALE *Notes on Nursing* vi. 39   Generally, the only rule of the private patient's diet is what the nurse has to give.

1914   A. BENNETT *Price of Love* xii. 256   In those days of State health insurance all doctors were too busy..to be of assistance to private patients.

1992   *Which?* Aug. 428/3   You may sometimes be better off in an NHS hospital, whether as an NHS patient or a private patient in a pay-bed.

private placement *n. Finance* (originally *U.S.*) the sale of stocks, bonds, or securities directly to a private investor (often without using an intermediary), rather than in a public offering; (also) stocks, etc., sold in this way.

1925   *N.Y. Times* 28 Mar. 21/3 (*heading*)   Kuhn, Loeb & Co..takes $4,735,000 railroad bonds for private placement.

1939   *N.Y. Times* 2 Nov. 33/3   From the short term this appears to give borrowers a great advantage in the private placement market, an advantage which they could never find in direct sales to the public.

1951   *Times* 24 Jan. 6/7   South Africa had also arranged for the private placement with eight American commercial banks of $10m. of the Union's promissory notes.

2000   *Red Herring* May 192/2   We haven't made any decision yet as to whether we'll go public; we've just made a desicion to issue a private placement.

private playhouse *n.* = PRIVATE HOUSE *n.* 2; (later also) any theatre owned and run by a private individual, *esp.* one staging performances for invited audiences only.

> 1609 T. DEKKER *Guls Horne-bk.* vi. 28 Whether therefore the gatherers of the publique or priuate Play-house stand to receiue the afternoones rent, let our Gallant (hauing paid it) presently aduance himselfe vp to the Throne of the Stage.

> 1795 M. CONCANEN & A. MORGAN *Hist. & Antiq. of Parish of St. Saviour's, Southwark* 200 Yet it should seem that persons were suffered to sit on the stage only in the private playhouses (such as Blackfriars &c.) where the audience was more select and of a higher class.

> 1829 J. H. REYNOLDS *One, Two, Three, Four, Five* I. ii. 18 I seek in vain for elegant recreation; no private play-houses, no debating society.

> 1910 *Mansfield (*Ohio*) News* 30 Aug. 2/7 Recently D'Annunzio gave a performance at the private playhouse of a friend of his in Paris.

> 1998 S. DAVID *Prince of Pleasure* (2000) v. 132 He spent more than £60,000 on a private playhouse in which he would indulge his passion for drama.

private practice *n.* work undertaken for a fee for a private client or patient; a privately run business which provides a service for paying clients; cf. sense A. 2b(b).

> 1724 *Philos. Trans. 1722–3* (Royal Soc.) **32** 213 The..Regard for the Good of Mankind, which you have always manifested, as well in your extensive private Practice as in that publick Post, which you have so long and so usefully fill'd, must affect you [etc.].

> 1843 R. J. GRAVES *Syst. Clin. Med.* ix. 99 In private practice the physician is called at an early period of the disease.

> 1945 *Fortune* Mar. 109/2 Tommy Corcoran, no longer part of the janissariat, is back in the law, with a private practice in Washington.

> 1967 *Brit. Jrnl. Psychiatry* **113** 1052/2 Private practice is simply a method of making a lucrative racket out of pampering or swindling those who can afford to pay.

> 2000 *Building Design* 18 Feb. 26/4 (*advt.*) Dynamic private practice with an established list of blue-chip clients requires proactive and driven professionals.

private press *n.* a small privately-owned printing and publishing house (now usually one issuing small print runs of books embodying higher standards of production than those of commercial publishers).

> 1643 in D. Neal *Hist. Puritans* (1855) 456/2 The Company of Stationers and the Committee of Examinations are required to make strict inquiry after private presses, and to search all suspected shops and warehouses for unlicensed books and pamphlets.

> 1687 A. BEHN *Luckey Chance* IV. i. 47 Then he keeps a private Press and prints your Amsterdam and Leyden Libels.

> 1834 J. MARTIN *Bibliogr. Catal. Bks. Privately Printed* p. v The second portion of the work, consisting of an account of the publications from literary clubs, and private presses.

> 1900 *Library* **1** 407 Since the days when Horace Walpole started as a master-printer at Strawberry Hill

quite a number of book-lovers have amused themselves with the management, and occasionally with the actual working, of a private press.

1993   *Dict. National Biogr.: Missing Persons* (BNC) 65/2   He published on American history and established his own private press, the Guyon House Press.

private property *n.* property owned by an individual person, company, etc.

1642   J. M. *Reply to Answer* 40   It must be agreed that the State hath an interest Paramount in every mans private property.

1760   C. Lennox *Lady's Museum* No. 7. 527   All matters of importance, or relative to private property, were to be laid before him.

1868   M. Pattison *Suggestions Acad. Organisation* §1. 7   A great deal of foolish bluster was talked about interference with private property.

1997   *Economist* 1 Feb. 57/1   If..the government decided to put a camp-ground on part of the private property, the group would first have to agree and then buy back the grazing rights from Mr Bass.

private residence *n.* = PRIVATE HOUSE *n.* 1.

1723   *Impartial Hist. Peter Alexowitz* 65   He pitch'd upon the place for his Retreat, or private Residence.

1797   A. Radcliffe *Italian* II. vii. 234   She hoped, therefore, that he had only been sent to some private residence belonging to his family.

1836   C. Dickens *Pickwick Papers* (1837) xxi. 222   At length, late one night, Heyling..appeared at his attorney's private residence, and sent up word that a gentleman wished to see him instantly.

1974   P. Lovesey *Invitation to Dynamite Party* iii. 34   'There was a second explosion..at Sir Watkin Wynn's residence.' 'A private residence? What have they got against Sir Watkin Wynn?'

1998   L. Forbes *Bombay Ice* (1999) 76   The family has to slum it on the top floor, but even so it's still the tenth largest private residence in the world.

private road *n.* a road maintained at private (rather than public) expense, to which public access may or may not be limited, (now) *esp.* one giving access to private property.

1652   G. Fidge *Wit for Mony* vii. sig. A6   Hind having gotten a good purchase in Gold past away the day very merrily, & towards night rides to an Inne which stood in a private Roade.

1775   *Edinb. Advertiser* 21 Apr.   Coming to a drawbridge..he desired that it might be immediately let down; but they refused; saying it was a private road, and that he had no authority to demand passage that way.

1838   R. S. Surtees *Jorrocks's Jaunts* 55   A private road and a line of gates through fields now greet the eyes of our M'Adamisers.

1903   *Times* 16 Mar. 4/2   The club decided to make an effort to obtain before next winter a private road, instead of using, as heretofore, the public road to Klosters.

2001   J. O'Brien *At Home in Heart of Appalachia* xiii. 204   At the end of the hardtop, I take a short trail to the private road that curves down to the telescopes.

private room *n.* (in a club, hotel, etc.) a room which may be hired for private use; (in a hospital) a room which affords privacy for a patient, *esp.* such a room provided on a fee-paying basis.

> 1797 T. Holcroft *Adventures Hugh Trevor* V. xi. 186   The place of meeting was a private room in a coffee-house.
>
> 1824 W. Scott *Redgauntlet* III. vii. 197   Walking into the inn, [he] demanded from the landlord breakfast and a private room.
>
> 1878 *Times* 21 Nov. 6/5   The 'No. 8' block, on the west of the hospital,..had the means of providing for upwards of 60 paying patients in wards and private rooms.
>
> 1920 'Sapper' *Bull-dog Drummond* 7   Have we ever had staying in the hotel a man called le Comte de Guy?.. Has he ever fed here, or taken a private room?
>
> 1994 R. Preston *Hot Zone* Ebola River 87   At the Ngaliema Hospital in Kinshasa, Nurse Mayinga had been put into a private room, which was accessible through a kind of entry room, a gray zone, where the nurses and staff were supposed to put on bioprotective gear before they entered.
>
> 1995 *Guardian* 16 Feb. I. 10/7   Karaoke parlours..comprise a warren of private rooms in which customers sing to the words of tunes played on television screens.

private school *n.* a fee-paying school run for the personal profit of the proprietors; a school which does not receive state funding and is not subject to the state education authority; (in quot. 1857) a preparatory school (cf. sense C. 6).

> 1574[1]Priuate schoole [see sense A. 2b(a)].
>
> 1676 *Cramond Kirk Session* II. 5 Nov.   Considereing how much the public schoole at the church is prejudged by privat schooles.
>
> 1751 *Mem. Lady of Quality* in T. Smollett *Peregrine Pickle* III. lxxxviii. 66   I was the only child of a man..who indulged me..with..paternal affection; and when I was six years old, sent me to a private school, where I stayed till my age was doubled.
>
> 1857 T. Hughes *Tom Brown's School Days* I. iii. 67   A private school, where he went when he was nine years old.
>
> 1914 C. Mackenzie *Sinister St.* II. III. iii. 547   I don't think it is snobbishness... It's a throw back to primitive life in a private school.
>
> 1997 *N.Y. Times Bk. Rev.* 29 June 24/1   Everdell..is dean of humanities at St. Ann's, a private school in Brooklyn, where he has taught history for 25 years.

private schoolmaster *n.* a personal tutor; a schoolmaster at a private school.

> 1588 W. Kempe *Educ. Children* sig. E4[v]   Some heere do counsell the Father to seeke out a priuat Schoolemaister for his child.
>
> a1691 R. Baxter *Reliquæ Baxterianæ* (1696) 96   A Man of great sincerity and zeal, and desire to do good, and devotedness to God,..falling into the Life of a private Schoolmaster.
>
> 1857 T. Hughes *Tom Brown's School Days* I. iii. 69   Were I a private schoolmaster.
>
> 1930 E. Waugh *Vile Bodies* viii. 143   My private schoolmaster used to say, 'If a thing's worth doing at all, it's

worth doing well.'

1988   R. Symonds *Alternative Saints* (BNC) 102   He remained in Wales as a private schoolmaster until he became chaplain and tutor to the family of Lord Carbery.

† **private seal** *n. Obsolete* = Privy seal *n.* 3a.

1440   *Chancery Proc.* Ser. C1 File 9 No. 447 (*MED*)   William Gargrave of Holme and Cristofere Banastre of Merton, Esquiers, haue ben ij tymes send for by the kyngis priuat seel at the Instaunce and costages of your said suppliaunt.

1531   in I. S. Leadam *Select Cases Court of Requests* (1898) 33   To graunte vnto your seid Orator your most dredd wrytte of pryuatte seale to be dyrected vnto the seid abbot.

private secretary *n.* *(a)* a secretary employed by a government minister, dealing with official correspondence, etc.; *(b)* a secretary in the employ of a particular individual, rather than of a society, department, etc.

1677   S. Pepys *Portugal Hist.* 76   Gaspar de Faria, private Secretary, by order of the King, put into his hands oftentimes papers of greatest Concerns.

1773   R. Jephson *Let.* 2 Mar. in D. Garrick *Private Corr.* (1831) I. 530   Our friend Tighe is much engaged in his office of Private Secretary to the Lord Lieutenant, but is getting better health and more strength every day.

1891   W. Fraser *Disraeli & his Day* (ed. 2) 42   Mr Algernon Greville became, some years afterwards, Private Secretary to the Duke.

1930   J. B. Priestley *Angel Pavement* v. 207   I can't bear those private secretary jobs. Yours is one of them, isn't it?

1991   *Sanity* Jan. 7/1   He became private (i.e. political) secretary to two government ministers in the Home Office.

private secretaryship *n.* the office or position of private secretary.

1789   *Hartly House, Calcutta* II. xx. 116   The peace-offering..was no less than an appointment to a private secretaryship.

1812   *Times* 16 Apr. 2/3   This private secretaryship, with the salary annexed, is an after-device.

1880   E. W. Hamilton *Diary* 25 Apr. (1972) I. 3   Horace Seymour and Henry Primrose are the two between whom the other private secretaryship lies.

1954   K. Amis *Lucky Jim* iv. 48   Our influencial friend will shortly be declaring his private secretaryship vacant.

1981   *Times* 25 Mar. 14/1   The interconnection of junior ministers and parliamentary private secretaryships is striking.

private sector *n.* that part of an economy, industry, etc., which is privately owned and free from direct state control.

1930   H. J. Stenning tr. A. Feiler *Russ. Exper.* 89   In this sphere the programme contemplates a determined

onslaught on the private sector for the benefit of the socialized, the nationalized, or the co-operative sector.

1996   *Outlook (*New Delhi*)* 28 Aug. 36/1   This year's Olympics taught the Americans that there's a flip side to relying solely on the private sector.

private service *n.* service to an individual rather than to the community, state, etc.; (in later use) *spec.* domestic service in a private house.

a1652   R. BROME *Eng. Moor* III. i. 39 in *Five New Playes* (1659)   And though I outwardly appear your Drudge, 'Tis fit I have a Maid for private service.

1718   R. SAMBER tr. C. Ancillon *Eunuchism Display'd* I. i. 7   He might have none to attend him in his private Service but Eunuchs.

1843   C. DICKENS *Martin Chuzzlewit* (1844) vii. 85   All them trades I thought of was a deal too jolly; there was no credit at all to be got in any of 'em. I must look for a private service... I might be brought out strong..in a serious family.

1934   D. L. SAYERS *Nine Tailors* 139   Deacon was a waiter in some club... He wanted to try private service.

1978   M. WARD & N. WARD *Home in Twenties & Thirties* 38/1   There was..an inexorable reduction in the number of people engaged in private service.

private ship of war *n.* now *historical* = PRIVATEER *n.* 1a; cf. *private man of war n.*

1702   tr. P. de la Court *True Interest Republick Holland & W.-Friesland* II. i. 207   Private Ships of War [were] by great Rewards perswaded to take and destroy the Enemys Ships.

1804   *Times* 3 May 3/3   Those beautiful private ships of war the *Sir Thomas Trowbridge*, of 16 guns, and the *Sir John Colpays*, of 14 guns..have been surveyed by the proper officers.

1988   P. O'BRIAN *Let. of Marque* i. 7   Stephen Maturin had bought her as a private ship of war, a letter of marque, to cruise upon the enemy.

private soldier *n.* an ordinary soldier of the lowest rank; = sense C. 10; cf. *common soldier n.* at COMMON *adj.* and *adv.* Compounds 2.

1566   W. PAINTER tr. O. Landi *Delectable Demaundes* III. f. 68   He knewe well that by his natiuitie, he was appointed to be generall of armies, and not a simple souldior: wherfore he behaued him selfe according to the Maiestie of that office, and not like a priuate souldior.

1579   L. DIGGES & T. DIGGES *Stratioticos* 152   They can doe no more than Privat Souldiors.

1698   *Mem. E. Ludlow* I. 192   Pretending..to keep the private soldiers, for they would no longer be called common soldiers, from running into greater extravagancies and disorders.

1760   C. JOHNSTONE *Chrysal* II. iv. 177   A man, in the habit of a private soldier, threw himself prostrate across his way, crying, 'Mercy! O great king! have mercy on the sufferings of a wretch in despair, and shew yourself the substitute of heaven by impartial justice.'

1898   E. J. HARDY in *United Service Mag.* Mar. 646   Another expression, which is far more objectionable [than the name 'Tommy Atkins'], is to speak of a 'common soldier' instead of a private soldier.

1992   G. M. FRASER *Quartered Safe out Here* p. xiv   I must emphasise that at private soldier level you

frequently have no idea where you are, or precisely how you got there, let alone why.

private trade *n.* trade carried on by an individual for his or her personal profit.

> [1601   J. Wheeler *Treat. Commerce* 46   Diuers of the Company had..erected vnto themselues a priuate, irregular, and stragling Trade.]
>
> 1612   J. Smith *Map of Virginia* 50   There was ten-times more care, to maintaine their damnable and private trade, then to provide for the Colony things that were necessary.
>
> 1736   H. Fielding *Pasquin* IV. i. 51   But Priests, and Lawyers, and Physicians made These general Goods to each a private Trade.
>
> 1821   G. Simpson *Jrnl.* 8 Jan. in *Publ. Hudson's Bay Rec. Soc.* (1938) I. 212   Chastellan & Lamallice..are renewing their old practice of carrying on Private Trade with the Indians.
>
> 1991   C. Anderson *Grain* p. i   The so-called 'private' companies—those companies in the hands of private trade as opposed to the farmer-owned wheat pools.

private trader *n.* a person who carries on trade for his or her personal profit.

> 1616   in W. Foster *Lett. received by E. India Co.* (1901) V. 119   With the intelligence concerning the private traders of Captain Downton's merchants.
>
> 1784   A. Smith *Inq. Wealth of Nations* (ed. 3) III. v. iii. 133   The competition of the two companies with the private traders..is said to have well nigh ruined both.
>
> 1830   J. F. Cooper *Water Witch* I. xi. 203   Prudence is a cardinal quality, in a private trader; and it is a quality that I esteem in Master Skimmer, next to his punctuality.
>
> 1991   *South* Aug. 95/4   From time to time the government tries to take the video-business in hand but it cannot compete against private traders.

private trading *n.* = *private trade n.*

> 1640   H. Mill *Nights Search* xlvii. 233   She keeps her private trading, To help at need; her husbands trade is fading.
>
> 1739   Ld. Hardwicke in *Rep. Cases Chancery* (1765) I. xci. 546   For the benefit of the Captain, who staid there six days merely for the sake of private trading.
>
> a1894   R. L. Stevenson *In South Seas* (1896) IV. vii. 369   Tembinok' had two brothers. One, detected in private trading, was banished.
>
> 1929   *Times* 26 Feb. 17/5   He courageously scrapped his own Bolshevist economic theories in 1921 and reinaugurated private trading.
>
> 1990   *Farmer's Weekly (*Perth*)* 11 Oct. 25/3 (*advt.*)   Private trading through Grain Pool Permits is possible for domestic consumption.

private treaty *n.* a form of property sale effected by a private agreement between the seller and a bidder, rather than by auction, public tender, etc.; see also quot. 1973.

1858   *Estates Gaz.* 16 Aug. 16/1 (*advt.*)   To be sold, by private treaty, a substantial and well-built house.

1922   V. SACKVILLE-WEST *Heir* i. 19   Are we to try for auction or private treaty? Personally I think the house at any rate will go by private treaty.

1973   P. WESTLAND & A. RODWAY *Place of your Own* i. 11/2   In Scotland..houses are more often sold 'by private treaty'. This way, the owner places a reserve, or 'upset' price on the property and invites those interested to make offers, in writing, by a specified date. On that date, the offers are examined, and the property will usually go to the highest bidder. An offer made this way is binding by law, unless you withdraw it before it is formally accepted... Some properties in England and Wales are offered for sale on these terms.

1988   *Home Finder* May 51/1   Ask the auctioneer if offers will be considered prior to auction, in other words, whether you can purchase by private treaty.

private view   *n.* a viewing (now esp. of an exhibition) to which the general public is not admitted; = *private viewing n.*

1706   T. D'URFEY *Wonders in Sun* III. 43   Ambassador from the Kingdom of the Birds; who, thro' Curiosity desiring a private View of you, and being gratify'd, has strangely accus'd ye of Murder upon one of the Brothers of Plumply Lord Pheasant.

1746   *N.Y. Evening Post* 29 Dec. (*advt.*)   If any Gentlemen or Ladies, hath a Mind to have a private View of the same, they may, by giving two Hours Warning before hand.

1862   W. SANDBY *Hist. Royal Acad. Arts* II. 240   The art-critics for the newspapers, etc., were admitted to the private view of the exhibition.

1996   *Independent* 14 Oct. I. 3/4   He is seen in the film coaching staff for the private view of the William Morris exhibition.

private viewer   *n.* a person attending a private viewing.

1897   *Daily News* 28 Apr. 6/6   The galleries..soon to be refilled by the critics, the private viewers, and the outside crowd.

1997   *Northern Echo* (Nexis) 19 Mar. 5   We aren't interested in private viewers who have a couple of pirates in their collection. We want to catch the big fish.

private viewing   *n.* = *private view n.*

1850   *Punch* **19** 88/2   As to the privilege of private views [of the Exhibition], the whole thing is a farce when compared with the privilege of private viewing claimed..by our young friends.

1898   *Westm. Gaz.* 28 Apr. 5/3   On the whole the private viewing ladies have had the excellent taste of coming in the morning in morning dress.

1965   *Observer* 28 Feb. 2/6   The occasion was the private viewing of the most important show of the New York art season.

2000   G. FYFE *Art, Power & Modernity* iv. 82   With its rituals of dining and private viewing, the RA and its Exhibition translated the status struggles of Victorian Society into the hierarchies of art.

private war   *n.* a war fought by a restricted number of participants from personal or private motives; also in extended use.

1548   *Hall's Vnion: Henry VII* f. lvii   He more detested & abhorred intestine and priuate warre, then death or any thynge more terrible.

a1599   E. SPENSER *View State Ireland* 197 in J. Ware *Two Hist. Ireland* (1633)   The English Lords and Gentlemen, who then had great possessions in Ireland, began thorough pride and insolency, to make private warres one against another.

1728   E. CHAMBERS *Cycl.* at *Treve de Dieu*   The Disorders and Licences of private Wars..oblig'd the Bishops of France to forbid such Violences within certain Times.

1866   C. M. YONGE *Dove in Eagle's Nest* I. p. vi   An offended nobleman, having sent a *Fehdebrief* to his adversary, was thenceforward at liberty to revenge himself by a private war.

1974   'G. BLACK' *Golden Cockatrice* xi. 194   A killing that was one incident in the continuing private war the Russians and the Chinese have been waging against each other.

1987   'J. GASH' *Moonspender* (1988) vii. 76   I don't believe that you..suddenly decide to recruit him in your private war with a load of moonspenders.

private ward *n.* a hospital ward, usually containing a single bed, that gives a patient privacy or is for fee-paying patients.

a1832   W. SCOTT *Surgeon's Daughter* vii, in *Waverley Novels* (1855) 498   Symptoms are dubious yet... That was an alarming swoon. You must have him carried into the private ward.

1935   D. L. SAYERS *Gaudy Night* ix. 191   He's in a private ward, so you can get in any time.

1960   C. WATSON *Bump in Night* i. 15   He lay in a small private ward of Chalmsbury General Hospital.

1991   J. SPOTTISWOODE *Undertaken with Love* (BNC) 73   He had apparently been..so disturbing the other patients that he had been moved, temporarily, to a private ward.

private wire *n. Telephony* *(a)* = *private line n.* (a); *(b)* a wire in an exchange used to test whether a line is in use without intrusion on a call in progress.

1852   Private wires [see sense A. 8b].

1878   *Telegr. Jrnl.* **6** 51/1   The regulations concerning the despatch and receipt of telegrams, the tariffs for the same, and for the renting of private wires.

1940   *War Illustr.* 16 Feb. p. ii/1   Taking the final proof of his commentary on the foreign news of the day to the 'private wire' room, to be telegraphed or telephoned to Manchester.

1969   S. F. SMITH *Telephony & Telegr. A* vi. 153   A third wire is therefore provided on all connexions through the exchange, the potential of which indicates the condition of the circuit. This avoids intrusion on calls in progress and is called the private wire, usually abbreviated to '*P-wire*'.

1998   *What Cellphone* Nov. 29/1   A further benefit is that a private wire system can be set up in such a way as [*sic*] a company's mobile phones effectively behave like extensions of the office switchboard.

private world *n.* the realm of personal thoughts, perceptions, interests, etc., within which one moves or lives; a person's private consciousness (frequently implying a degree of fantasy or isolation from the real world).

1873   T. HARDY *Pair of Blue Eyes* I. xi. 234   It was the first time that she had had an inner and private world

apart from the visible one about her.

1921   A. HUXLEY *Crome Yellow* xiii. 128   He determined to retire absolutely from it [*sc.* the great world] and to create..at Crome a private world of his own.

1989   G. DALY *Pre-Raphaelites in Love* vi. 250   Ned retreated into a private world of his own making.

Democrats: Google must protect privacy of abortion patients

By BARBARA ORTUTAY

More than 40 Democratic members of Congress are asking Google to stop what they see as the unnecessary collection and retention of people's location data, arguing the information could be used to identify women seeking abortions.

In a letter sent Tuesday to Sundar Pichai, the CEO of Google parent Alphabet Inc., the lawmakers express concern that if abortion were to become illegal in the U.S., the company's "current practice of collecting and retaining extensive records of cell phone location data will allow it to become a tool for far-right extremists looking to crack down on people seeking reproductive health care."

If the Supreme Court upends the 1973 decision that legalized abortion — as a draft opinion suggests it may in the coming weeks — pregnancies could be surveilled and the data shared with police or sold to vigilantes, privacy experts fear.

Google, specifically, stores "historical location information about hundreds of millions of smartphone users," the letter notes, "which it routinely shares with government agencies."

Representatives for Alphabet did not immediately respond to a message for comment. Tech companies have largely tried to stay out of the abortion debate. Meta Platforms, which owns Facebook, has reportedly reminded employees that they are prohibited from discussing abortion in workplace communication channels. Meta did not respond to a request for comment.

In their letter, the Democrats, who were led by Sen. Ron Wyden from Oregon, asks Google to stop collecting and keeping records of their customers' every movement.

Law enforcement officials routinely obtain court orders forcing Google to turn over its customers' location information, the letter notes. This includes "geofence" orders, which are requests for Google to provide data about everyone who was near a specific location at a specific time.

Google received 11,554 geofence warrants in 2020, according to the company. It has not said how many of those it complied with.

Better understand and reach your customers with new Cross Device capabilities in Google Analytics

Jesse Savage

Today, we're introducing new Cross Device features to Google Analytics. Analytics will now help you understand the journey your customers are taking across their devices as they interact with your website, giving you a complete view of the impact of your marketing so you can run smarter campaigns that deliver more tailored experiences to your customers.

Piecing together a more complete picture

Cross Device reporting in Analytics takes into account people who visit your website multiple times from different devices. Now, instead of seeing metrics in Analytics that show two separate sessions (e.g., one on desktop and the other on mobile), you'll be able to see when users visited your website from two different devices. By understanding these device interactions as part of a broader customer experience, you can make more informed product and marketing decisions.

Say you're a marketer for a travel company. With the new Acquisition Device report, you may find that a lot of your customers first come to your website on mobile to do their initial research before booking a trip later on desktop. Based on that insight, you might choose to prioritize mobile ad campaigns to reach people as they start to plan their trip.

In addition to the Acquisition Device report, you'll soon have access to other Cross Device reports like Device Overlap, Device Paths and Channels. Our Cross Device reports only display aggregated and anonymized data from people who have opted in to personalized advertising (as always users can opt out at any time).

Reaching the right customers along the way

Analytics will also now help you create smarter audiences based on the actions people take on various devices. That way you can deliver more relevant and useful experiences.

Let's say you're a shoe retailer and you want to share a special promotion with your most loyal customers. You decide this means people who have purchased more than $500 in shoes on your website in the last 12 months using any of their devices. If a group of customers buy $300 worth of shoes on their phone and another $300 on their desktop, they're just as valuable as another group who spend $600 on a single device, right?

Analytics now understands that these two groups of customers actually spent the same amount on your website, helping you create a more accurate audience list to reach the right customers. And spend isn't the only way to segment and build audiences. You can also create remarketing campaigns to reach audiences based on how many times they visit your website across multiple devices.

Get started

To use these new Cross Device features, start by visiting the Admin section of your Analytics account and choose the setting to activate Google signals. (If you don't see this setting, you will soon—we'll roll it out to all Analytics accounts over the coming weeks.) There's no need to update your website code or get additional assistance from a developer.

With these new beta features in Analytics, we hope you'll quickly see that by better understanding the customer journey across devices, you can create more relevant and useful experiences for your customers.

Google's Eric Schmidt Calls Julian Assange 'Paranoid' and Says Tim Cook Is Wrong

Google's executive chairman complains about Julian Assange, Tim Cook and data.

By **NICOLE SAWYER**
September 23, 2014, 1:02 PM • 4 min read

0:43

Eric Schmidt's Message To Tim Cook

Watch Google's Chairman with Rebecca Jarvis on Real Biz
ABC Real Biz with Rebecca Jarvis

— -- Eric Schmidt, Google's executive chairman, spent more than a decade as the Google's CEO, taking the company from a startup to a global tech giant. He spoke with ABC News' Real Biz about disagreements with Apple CEO Tim Cook, this whole privacy thing and why he thinks WikiLeaks' Julian Assange is "paranoid."

Schmidt teamed up with former product chief Jonathan Rosenberg to pen a book called "How Google Works," released today by Grand Central Publishing. Rosenberg joined Google in 2002 and managed search, ads, Gmail, Android, apps, and Chrome and today is an adviser to Google's co-founder Larry Page.

Google has won the top spot in Fortune's list of "Best Companies" five times, and is one of the stalwarts of Silicon Valley innovation, with Google Glass, driverless cars and, of course, those money-making ads.

Schmidt and Rosenberg's book focuses on the management of Google, revealing Schmidt's leadership secrets of how to get everyone on your management team to agree on a big decision.

In an interview with ABC News' chief business correspondent Rebecca Jarvis, Schmidt said: "You need buy-in and you need ownership for whatever the corporation is going to do," to avoid the "bobble head" effect in which "everybody goes yes and then the moment they leave the table, they go and they fight against you."

"Start your staff meeting by asking everyone their opinion and making sure everyone speaks," he suggested.

Instead of beginning the meeting with the most senior head honcho in the room dominating the conversation, he said it's important to get a discussion going from all of the people involved in the meeting to make sure the best idea comes out as fast as it can and then "set a deadline."

The Mountain View, California-based company is not only famous for its decision making, it's also known for its sneaker-wearing culture of co-founders Larry Page and Sergey Brin, and their motto, "Don't be evil." But Schmidt's book reminds readers that Google is indeed a mammoth, global corporation.

Top Stories

Car linked to escaped inmate, corrections officer found
1 hour ago

Judge rules GOP Rep. Marjorie Taylor Greene can stay on ballot
1 hour ago

Parents face backlash after 6-year-old allowed to run full marathon
May 06, 9:06 AM

Daunte Wright's mother detained after recording traffic stop
4 hours ago

Barry Morphew and daughters speak out for 1st time since murder charges were dropped
May 06, 8:04 AM

● ABC News Live

24/7 coverage of breaking news and live events

The C-Suite Insider: Google's Eric Schmidt Wakes Up at 8 AM

Google Seeks Help Defining 'Right to Be Forgotten'

Google's EU Antitrust Woes Extended

Speaking with ABC News, Schmidt addressed a recent comment by Apple CEO Tim Cook that for Internet companies, "You're the product." While Cook didn't address Google by name, he criticized firms that "build a profile based on your email content or Web browsing habits to sell to advertisers."

"I think that's not quite right," Schmidt said of Cook's letter published last week. "The fact of the matter is Google allows you to delete the information that we know about you and in fact, Google is so concerned about privacy that you could in fact, if you're using Chrome for example, you can browse in what is called 'incognito mode' where no one sees anything about you. So I just don't think that's right."

Days ago, WikiLeaks founder Julian Assange told the BBC and Sky News that, "Google's business model is to spy," and that the tech firm's "behavior" is "a privatized version of the [National Security Agency]."

Though Assange prefaced that Google is not acting illegally.

Schmidt took a poke back at Assange's comments, saying, "Well, he's, of course, writing from the, shall we say, luxury lodgings of the local embassy in London. The fact of the matter is Julian is very paranoid about things and it's true that the NSA did things that they shouldn't have done, but Google has done none of those things. Google never collaborated with NSA and in fact, we've fought very hard against what they did and since what the NSA did which we do not like, we have taken all of our data, all of our exchanges, and we fully encrypted them so no one can get them, especially the government."

⊡ Comments (0)   ⬜ 🐦 ✉

abcNEWS

Digital Content Next

DIGITAL CONTENT NEXT

Google Data Collection

—NEW—

August 2018

digitalcontentnext.org

Google Data Collection

Professor Douglas C. Schmidt, Vanderbilt University

August 15, 2018

I.   EXECUTIVE SUMMARY

1.   Google is the world's largest digital advertising company.[1] It also provides the #1 web browser,[2] the #1 mobile platform,[3] and the #1 search engine[4] worldwide. Google's video platform, email service, and map application have over 1 billion monthly active users each.[5] Google utilizes the tremendous reach of its products to collect detailed information about people's online and real-world behaviors, which it then uses to target them with paid advertising. Google's revenues increase significantly as the targeting technology and data are refined.

2.   Google collects user data in a variety of ways. The most obvious are "active," with the user directly and consciously communicating information to Google, as for example by signing in to any of its widely used applications such as YouTube, Gmail, Search etc. Less obvious ways for Google to collect data are "passive" means, whereby an application is instrumented to gather information while it's running, possibly without the user's knowledge. Google's passive data gathering methods arise from platforms (e.g. Android and Chrome), applications (e.g. Search, YouTube, Maps), publisher tools (e.g. Google Analytics, AdSense) and advertiser tools (e.g. AdMob, AdWords). The extent and magnitude of Google's passive data collection has largely been overlooked by past studies on this topic.[6]

3.   To understand what data Google collects, this study draws on four key sources:

   a.   Google's My Activity[7] and Takeout[8] tools, which describe information collected during the use of Google's user-facing products;

   b.   Data intercepted as it is sent to Google server domains while Google or 3rd-party products are used;

   c.   Google's privacy policies (both general and product-specific); and

   d.   Other 3rd-party research that has examined Google's data collection efforts.

4.   Through the combined use of above resources, this study provides a unique and comprehensive view of Google's data collection approaches and delves deeper into specific types of information it collects from users. This study highlights the following key findings:

---

[1] "Google and Facebook tighten grip on US digital ad market," *eMarketer*, Sept. 21, 2017, available at
https://www.emarketer.com/Article/Google-Facebook-Tighten-Grip-on-US-Digital-Ad-Market/1016494
[2] "Market share or leading internet browsers in the United States and worldwide as of February 2018," *Statista,* February 2018, available at https://www.statista.com/statistics/276738/worldwide-and-us-market-share-of-leading-internet-browsers/
[3] "Global OS market share in sales to end users from 1st quarter 2009 to 2nd quarter 2017," *Statista*, August 2017, available at https://www.statista.com/statistics/266136/global-market-share-held-by-smartphone-operating-systems/
[4] "Worldwide desktop market share of leading search engines from January 2010 to October 2017," *Statista,* Feb. 2018, available at https://www.statista.com/statistics/216573/worldwide-market-share-of-search-engines/
[5] Google 10K filings with the SEC, 2017, available at https://abc.xyz/investor/pdf/20171231_alphabet_10K.pdf
[6] Please see Appendix section IX.F for a list of past studies/news reports on Google data collection
[7] "My Activity," *Google*, available at https://myactivity.google.com/myactivity
[8] "Download your data," *Google*, available at https://takeout.google.com/settings/takeout?pli=1

a. Google learns a great deal about a user's personal interests during even a single day of typical internet usage. In an example "day in the life" scenario, where a real user with a new Google account and an Android phone (with new SIM card) goes through her daily routine, Google collected data at numerous activity touchpoints, such as user location, routes taken, items purchased, and music listened to. Surprisingly, Google collected or inferred over two-thirds of the information through passive means. At the end of the day, Google identified user interests with remarkable accuracy.

b. Android is a key enabler of data collection for Google, with over 2 billion monthly active users worldwide.[9] While the Android OS is used by Original Equipment Manufacturers (OEMs) around the world, it is tightly connected with Google's ecosystem through Google Play Services. Android helps Google collect personal user information (e.g. name, mobile phone number, birthdate, zip code, and in many cases, credit card number), activity on the mobile phone (e.g. apps used, websites visited), and location coordinates. In the background, Android frequently sends Google user location and device-related information, such as apps usage, crash reports, device configuration, backups, and various device-related identifiers.

c. The Chrome browser helps Google collect user data from both mobile and desktop devices, with over 2 billion active installs worldwide.[10] The Chrome browser collects personal information (e.g. when a user completes online forms) and sends it to Google as part of the data synchronization process. It also tracks webpage visits and sends user location coordinates to Google.

d. Both Android and Chrome send data to Google even in the absence of *any* user interaction. Our experiments show that a dormant, stationary Android phone (with Chrome active in the background) communicated location information to Google 340 times during a 24-hour period, or at an average of 14 data communications per hour. In fact, location information constituted 35% of all the data samples sent to Google. In contrast, a similar experiment showed that on an iOS Apple device with Safari (where neither Android nor Chrome were used), Google could not collect any appreciable data (location or otherwise) in the absence of a user interaction with the device.

e. After a user starts interacting with an Android phone (e.g. moves around, visits webpages, uses apps), passive communications to Google server domains increase significantly, even in cases where the user did not use any prominent Google applications (i.e. no Google Search, no YouTube, no Gmail, and no Google Maps). This increase is driven largely by data activity from Google's publisher and advertiser products (e.g. Google Analytics, DoubleClick, AdWords)[11]. Such data constituted 46% of all requests

---

[9] Dave Burke, "Android: celebrating a big milestone together with you," *Google,* May 17, 2017, available at
https://www.blog.google/products/android/2bn-milestone/
[10] Frederic Lardinois, "Google says there are now 2 billion active Chrome installs," *TechCrunch,* Nov. 10, 2016, available at
https://techcrunch.com/2016/11/10/google-says-there-are-now-2-billion-active-chrome-installs/
[11] Google recently rebranded AdWords as "Google Ads" and DoubleClick as "Google Ad Manager"

to Google servers from the Android phone. Google collected location at a 1.4x higher rate compared to the stationary phone experiment with no user interaction. Magnitude wise, Google's servers communicated 11.6 MB of data per day (or 0.35 GB/month) with the Android device. This experiment suggests that even if a user does not interact with any key Google applications, Google is still able to collect considerable information through its advertiser and publisher products.

f.   While using an iOS device, if a user decides to forgo the use of *any* Google product (i.e. no Android, no Chrome, no Google applications), and visits only non-Google webpages, the number of times data is communicated to Google servers still remains surprisingly high. This communication is driven purely by advertiser/publisher services. The number of times such Google services are called from an iOS device is similar to an Android device. In this experiment, the total magnitude of data communicated to Google servers from an iOS device is found to be approximately half of that from the Android device.

g.   Advertising identifiers (which are purportedly "user anonymous" and collect activity data on apps and 3rd-party webpage visits) can get connected with a user's Google identity. This happens via passing of device-level identification information to Google servers by an Android device. Likewise, the DoubleClick cookie ID (which tracks a user's activity on the 3rd-party webpages) is another purportedly "user anonymous" identifier that Google can connect to a user's Google Account if a user accesses a Google application in the same browser in which a 3rd-party webpage was previously accessed. Overall, our findings indicate that Google has the ability to connect the anonymous data collected through passive means with the personal information of the user.

4

Contents

II.   A DAY IN THE LIFE OF A GOOGLE USER

5.   To illustrate the multitude of touchpoints between Google and an individual, as well as the extent of information collected during these interactions, an experiment was designed where a researcher carried an Android mobile phone device[12] during a day's activities. The mobile phone was wiped by conducting a factory data reset[13] and configured as a new device to avoid prior user information associated with the device.[14] A new Google account was created (username "Jane"), so that Google had no prior knowledge of the user and had no advertising interests associated with the account. Researcher then went about a normal day using the mobile phone associated with the new Google account.

6.   The data collected by Google was checked using two tools provided by Google: My Activity[15] and Takeout.[16] The My Activity tool shows data collected by Google from any Search-related activities, use of Google applications (e.g. YouTube video plays, Maps search, Google Assistant), visits to 3rd-party web pages (while logged in to Chrome), and clicks on advertisements. The Google Takeout tool provides a more comprehensive information about all historical user data collected via Google's applications (e.g. it contains all past email messages on Gmail, search queries, location collection, and YouTube videos watched). We synthesized the collected data and used it to depict key information collection events in the form of a "day in the life" of the user "Jane," as shown in Figure 1.

7.   In the activity shown in Figure 1, as well as throughout the rest of this document, the collected data is categorized in two broad subgroups: *active* and *passive*. Active data is defined as information directly exchanged between the user and a Google product, whereas passive data is defined as information exchanged in the background without any obvious notification to the user. An example of active data collection occurred when Jane submitted a keyword in the Search tool bar and that search query was collected by Google. An example of passive data collection occurred when Jane's location was sent to Google after she entered a search query.

---

[12] LG X Power device with Android 6.0 version installed

[13] The factory data reset deletes all login data for Google services and other accounts, system and app data and settings, all downloaded apps, digital rights management licenses, music, images, documents and backups, and other usage data from the internal storage of the device.

[14] Researchers used LG X Power device that was wiped clean to the default factory settings and given new SIM card in order to ensure that no data was stored on the phone and that phone numbers could not be linked with any past usage.

[15] "My Activity," Google, available at https://myactivity.google.com/myactivity

[16] "Download your data," Google, available at https://takeout.google.com/settings/takeout?pli=1

Figure 1: Day in the life of Jane, highlighting touchpoints where Google collects data

A DAY IN THE LIFE OF A TYPICAL GOOGLE USER

MORNING ACTIVITY

1. Gets ready in the morning while listening to Google Play Music

2. Drops kids off at daycare before commuting to work

3. Checks the news while commuting to work on the subway

4. Searches for cold medicine while on the subway

AFTERNOON ACTIVITY

5. Walks from subway to work

6. Uses Maps to find a new lunch spot

7. Gets coffee from Starbucks using her Starbucks app

8. Schedules doctors appointment, Google creates a Calendar event from the confirmation email

9. Walks to Walgreens and purchases cold medicine using Google Pay

EVENING ACTIVITY

10. Takes an Uber home from work

11. Looks for hotels on Expedia for a weekend trip

12. Uses Google Home to play music for her kids

13. Watches late night TV videos on YouTube

cnn.com — Visited CNNPolitics - Political News, Analysis and Opinion

wsj.com — Visited California Takes Big Step to Require Solar on New Homes - WSJ

Search — Searched for cold symptoms
Search — Searched for cold vs allergies
Search — Searched for cold medicine

DUANE READE #14480 — $12.99
DATE May 9   TIME 6:50 PM
CARD USED Visa ••••1041

Web site tracking tools
`<script async id="tealium-tag-7110" src="//www.google-analytics.com/analytics.js"></script>`
`<iframe src="https://bid.g.doubleclick.net/xbbe/pixel?d=KAE" style="display: none;"></iframe>`

Assistant — Said play lullaby — PLAY — 9:25 PM • Details
Assistant — Said lower the volume — PLAY — 9:25 PM • Details

Item details
YouTube — Watched Jimmy Fallon Recaps the Met Gala The Tonight Show Starring Jimmy Fallon
Details — Today at 10:19 PM

8

8.   Analysis of key touch points during a normal day in the life of Jane suggested that the number of "passive" data collection events outnumbered the "active" events by approximately two-to-one (a detailed breakdown of characterization of active vs passive data collected appears in Table 3 of the Appendix section IX. A).

9.   Google analyzes the collected data to assess user interests, which it then applies to target users with appropriate ads. For example, Google provides a list of interests that it has inferred from a user's activities, available via the "topics you like" section in the Google's Ad Personalization webpage.[17] Figure 2 shows such a list that Google associated with Jane's account after a day's worth of activity. In total, Google attributed 18 interests to Jane, eight of which (shown by colored borders) closely matched Jane's usage and activities.[18]

Figure 2: Google's assessment of Jane's interest at the end of the day
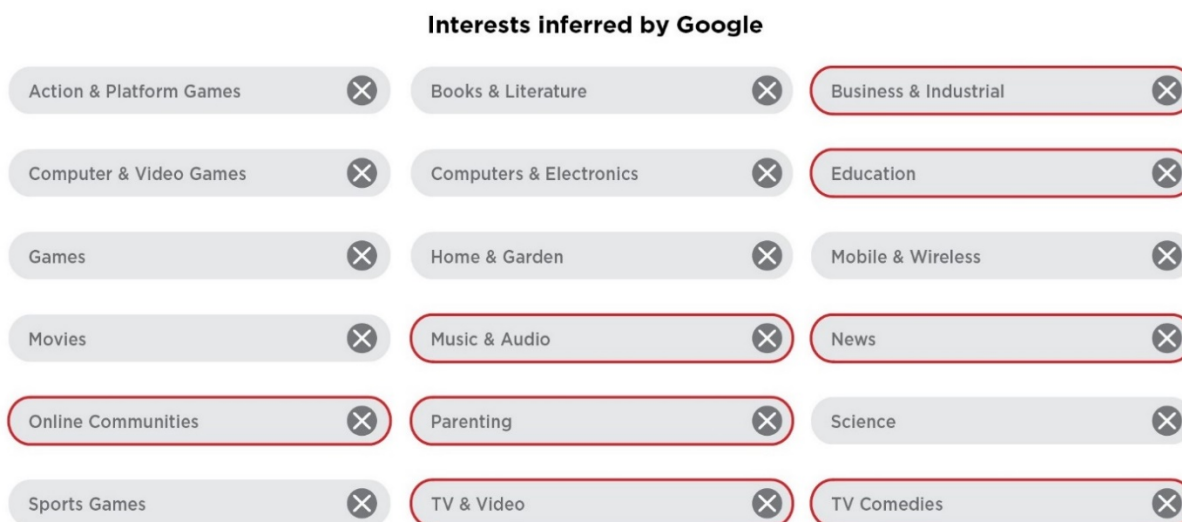
10.   Although My Activity and Takeout tools are helpful in assessing the amount of active data collected after a user interacts with Google's products, they do not paint a complete picture of the size and scale of Google's data collection. A comprehensive understanding of which requires a review of Google's product-specific privacy policies, as well as analyses of the actual data traffic passed to Google servers during the instances of a user's interaction with its services. Results derived from these resources are covered later in this report.

III.   DATA COLLECTION THROUGH ANDROID AND CHROME PLATFORMS

---

[17] "Ads personalization," *Google*, last accessed on August 15 2018, available at https://adssettings.google.com/authenticated
[18] It's unclear as to why other interests that have no connection with Jane's activities during the day show up in this list, though perhaps Google uses historical analysis of similar interests from other users to create associated recommendations.

11.   Android and Chrome are Google's key platforms that aid in significant user data collection due to their extensive reach and frequency of usage. By January 2018, Android captured 53% of the total US mobile OS market (Apple iOS held 45%)[19] and as of May 2017 there were more than 2 billion monthly active Android devices worldwide.[20]

12.   Google's Chrome browser held more than 60% share of all internet browser usage in the world with over 1 Billion monthly active users as reported in the 2017 Q4 10K filing.[21] Both platforms facilitate the use of Google and 3rd-party content (e.g. 3rd-party websites and 3rd-party apps) and hence provide Google access to a wide range of personal, web activity, and location information.

A.   Personal information and activity data collection

13.   To download and use apps from Google Play Store on an Android device, a user must have (or create) a Google Account, which becomes a key gateway through which Google collects personal information, including user name, email, and phone number. If a user registers for services such as Google Pay[22], Android also collects the user's credit card information, zip code, and birth date. All this information becomes part of a user's personal information associated with their Google Account.

14.   While Chrome does not mandate sharing additional personal information gathered from users, it does have the capability to capture such information. For example, Chrome collects a range of personal information via its form "autofill" feature, and such form fields typically include user name, address, phone number, login name, and passwords.[23] Chrome stores form fill information on a user's local drive, however, if the user logs in to Chrome using Google Account and enables its "Sync" feature, this information gets sent to and stored on Google servers. Chrome could also learn about the language(s) a person speaks during their interactions with its translate feature, which is enabled by default.[24]

15.   In addition to personal data, both Chrome and Android send Google information about a user's web browsing and mobile app activities, respectively. Any webpage visit is automatically tracked and collected under

---

[19] "Subscriber share held by smartphone operating systems in the United States from 2012 to 2018," *Statista,* May 2018, available at https://www.statista.com/statistics/266572/market-share-held-by-smartphone-platforms-in-the-united-states/
[20] Dave Burke, "Android: celebrating a big milestone together with you," *Google,* May 17, 2017, available at https://www.blog.google/products/android/2bn-milestone/
[21] Google 10K filings with the SEC
[22] "Google Chrome privacy whitepaper," *Google,* March 6, 2018, available at https://www.google.com/chrome/privacy/whitepaper.html#payments
[23] "Google Chrome privacy whitepaper," *Google,* March 6, 2018, available at https://www.google.com/chrome/privacy/whitepaper.html#autofill
[24] "Google Chrome privacy whitepaper," *Google,* March 6, 2018, available at https://www.google.com/chrome/privacy/whitepaper.html#translate

user credentials by Google if the user is signed in to Chrome. Chrome also collects information about a user's browsing history, passwords, website-specific permissions, cookies, download history, and add-on data.[25]

16.   Android sends periodic updates to Google servers, including device type, cell service carrier name, crash reports, and information about apps installed on the phone.[26] It also notifies Google whenever any app is accessed on the phone (e.g. Google knows when an Android user accesses their Uber app).

B.   User location data collection

17.   Android and Chrome platforms meticulously collect user location and movement information using a variety of sources, as depicted by Figure 3. For example, a "coarse location" assessment can be done by using GPS coordinates on an Android phone or through a network's IP address on a desktop/laptop device. The user location accuracy can be improved further ("fine location") through the use of nearby cell tower IDs or via scanning the device-specific BSSIDs or basic service set identifiers, assigned to the radio chipset used in nearby Wi-Fi access points.[27] Android phones can also use information from the Bluetooth beacons registered with Google's Proximity Beacon API.[28] These beacons not only provide user's geolocation coordinates, but could also pinpoint exact floor levels in buildings. [29]

Figure 3: Android and Chrome use multiple ways to locate a mobile user

---
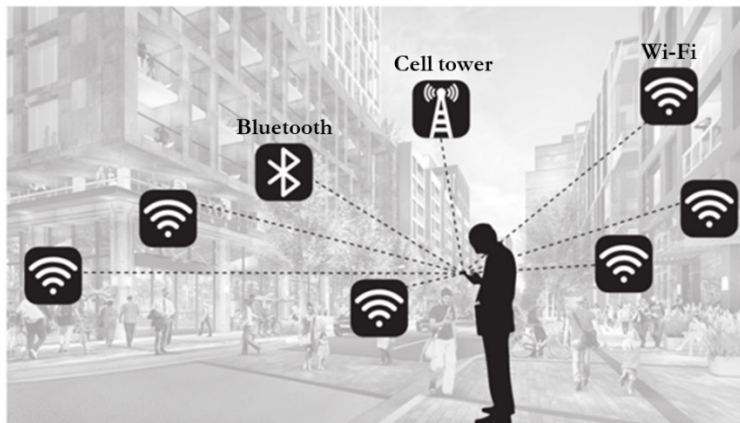
[25] "Google Chrome Privacy Notice," *Google*, March 6, 2018, available at https://www.google.com/intl/en/chrome/browser/privacy
[26] https://policies.google.com/privacy?hl=en&gl=us#infocollect
[27] To understand how location data is sent to Google servers in more depth, our researchers analyzed the data traffic from a mobile phone from a user in motion, applying the method described in Appendix section VIII.C.
[28] "Google beacon platform, proximity beacon API," *Google,* last accessed on August 15 2018, available at https://developers.google.com/beacons/proximity/guides
[29] "Google beacon platform, proximity beacon API," *Google,* last accessed on August 15 2018, available at https://developers.google.com/beacons/proximity/guides

18.   It's hard for an Android mobile user to "opt out" of location tracking. For example, on an Android device, even if a user turns off the Wi-Fi, the device's location is still tracked via its Wi-Fi signal. To prevent such tracking, Wi-Fi scanning must be explicitly disabled in a separate user action, as shown in Figure 4.

Figure 4: Android collects data even if Wi-Fi is turned off by user
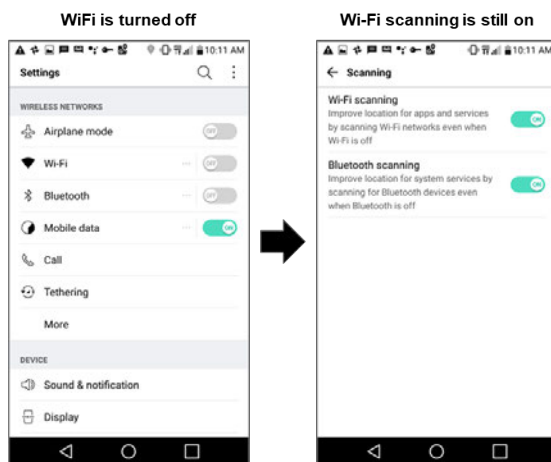
19.   The ubiquity of Wi-Fi hubs has made location tracking quite frequent. For example, during a short 15-minute walk around a residential neighborhood, an Android device sent nine location requests to Google. The request collectively contained ~100 unique BSSIDs of public and private Wi-Fi access points.

20.   Google can ascertain with a high degree of confidence whether a user is still, walking, running, bicycling, or riding on a train or a car. It achieves this by tracking an Android mobile user's location coordinates at frequent time intervals in combination with the data from onboard sensors (such as an accelerometer) on mobile phones. Figure 5 shows an example of such data communicated with the Google servers while the user was walking.

Figure 5: Snapshot from a Google user location upload

```
"activityReadings": [
    {
        "activities": [
            {
                "confidence": 99,
                "type": "onFoot"
            },
            {
                "confidence": 99,
                "type": "walking"
            },
            {
                "confidence": 1,
                "type": "unknown"
            }
        ],
        "timestampMs": 1527095517507
    },
```

C.   An assessment of passive data collection by Google through Android and Chrome

21.   Active data that Android or Chrome platforms collect and send to Google as a result of users' activities on these platforms can be assessed through the MyActivity and Takeout tools. Of potentially greater interest, however, is the passive data that these platforms collect, which goes beyond location data and which remains relatively unrecognized by the users. To assess the type and frequency of occurrence of such collection in greater detail an experiment was conducted that monitored traffic data sent to Google from mobile phones (both Android and iPhone) using the method discussed in Section IX.D in the Appendix. For comparison's sake, this experiment also included the analysis of data sent to Apple via an iPhone device.

22.   For simplicity, the phones were kept stationary, with no user interaction. On the Android phone a single Chrome browser session remained active in the background, whereas on the iPhone the Safari browser was used. This configuration provided an opportunity for systematic analysis of the background collection that Google performs purely through Android and Chrome, as well as collection that occurs in the absence of those (i.e. from iPhone device), without any additional collection requests generated by other products and applications (e.g. YouTube, Gmail, App usage).

23.   Figure 6 shows a summary of the results obtained from this experiment. The x-axis indicates the number of times the phones communicated with Google (or Apple) servers, whereas the y-axis indicates the phone type (Android or iPhone) and server domain type (Google or Apple) with which data packets were exchanged by the phones. The colored legend describes the broad categorization of the type of data requests identified by the domain address of the server. A complete list of domain addresses belonging within each category appears in Table 5 of Section IX.D of the Appendix.

13

24.   During a 24-hour time period the Android device communicated ~900 data samples to a variety of Google server endpoints. Of these, ~35% (or approximately 14/hour) were location-related. Google ad domains received only ~3% of the traffic, which is mainly due to the fact that the mobile browser was not actively used during the collection period. The remaining ~62% of communications with the Google server domains were roughly divided between requests to Google's Play App store, Android's uploads of device-related data (such as crash reports and device authorization), and other data which were predominantly in the category of Google services background calls and refreshes.

Figure 6: Traffic data sent from idle Android and iPhone mobiles
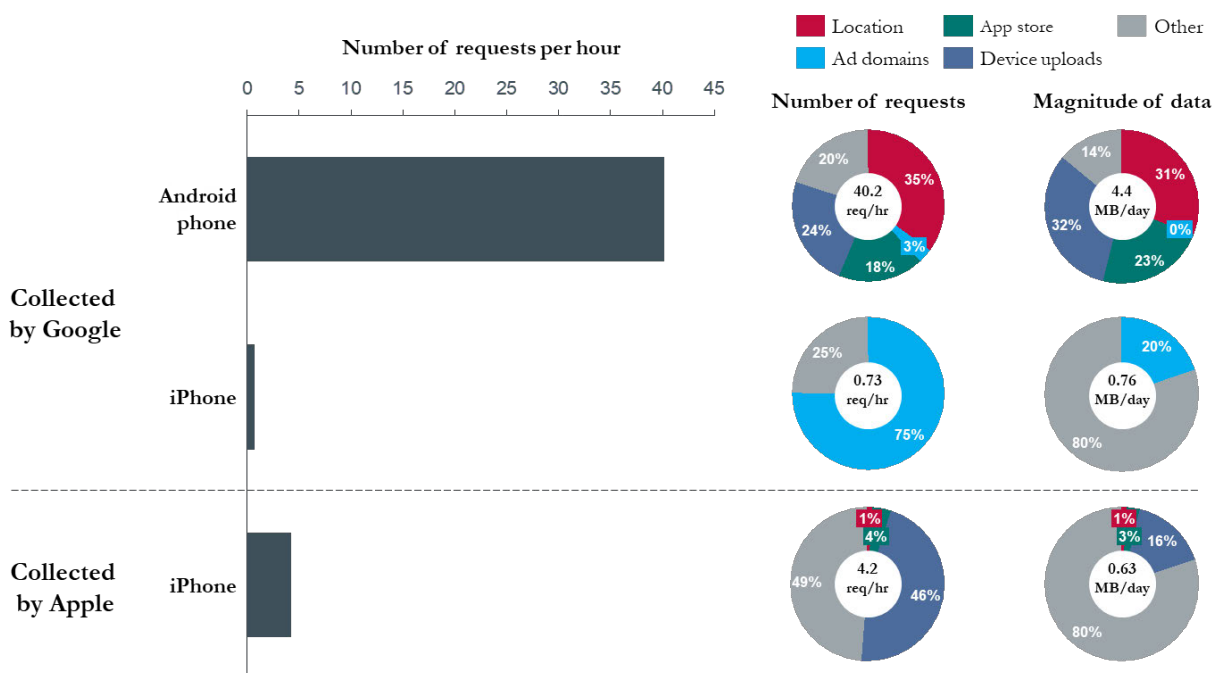
25.   Figure 6 shows that the iPhone device communicated with Google domains at more than an order of magnitude (~50x) lower frequency than the Android device, and that Google did not collect any user location during the 24-hour experiment timeframe via iPhone. This result highlights the fact that the Android and Chrome platforms play an important role in Google's data collection.

26.   Additionally, the iPhone device's communication with Apple's servers were 10x less frequent than the Android device's communications with Google. Location data made up a very small fraction (~1%) of the net data sent to Apple servers from the iPhone, with Apple receiving location-related communications once every day on an average.

27.   Magnitude wise, Android phones communicated 4.4 MB of data per day (~130MB per month) with Google servers, which is 6x more than what Google servers communicated through the iPhone device.

14

28.   As a reminder, this experiment was conducted using a stationary phone with no user interaction. As a user becomes mobile and starts interacting with their phone, the frequency of communications with Google's servers increases considerably. Section V of this report summarizes results from such an experiment.

IV.   DATA COLLECTION THROUGH PUBLISHER AND ADVERTISER TECHNOLOGIES

29.   A major source for Google's user activity data collection stems from its publisher- and advertiser-focused tools, such as Google Analytics, DoubleClick, AdSense, AdWords, and AdMob. These tools have tremendous reach, e.g. over 1 million mobile apps use AdMob,[30] over 1 million advertisers use AdWords,[31] over 15 million websites use AdSense,[32] and over 30 million websites use Google Analytics.[33]

30.   During the writing of this report Google rebranded AdWords as "Google Ads" and DoubleClick as "Google Ad Manager", however there were no changes instituted in the core product functionalities including information collection by these products.[34] Therefore, for the purpose of this report the names are kept unchanged to avoid confusion that may occur with related domain names (such as doubleclick.net).

31.   There are two main groups of users of Google's publisher- and advertiser-focused tools:

o   *Website and app publishers*, which are organizations that own websites and create mobile apps. These entities use Google's tools to (1) make money by allowing the display of ads to visitors on their websites or apps, and (2) better track and understand who is visiting their websites and using their apps. Google's tools place cookies and run scripts in the browsers of website visitors that help determine a user's identity, track their interest in content, and follow their online behavior. Google's mobile app libraries track use of apps on mobile phones.

o   *Advertisers*, which are organizations that pay to have banner, video, or other ads delivered to users as they browse the Internet or use apps. These entities apply Google's tools to target specific profiles of people for advertisements to increase the return on their marketing investments (better targeted ads generally yield higher click-through rates and conversions). Such tools also enable advertisers to analyze their audiences and measure the efficacy of their digital advertising by tracking which ads were clicked with what frequency and by providing insight into the profiles of people who clicked on ads.

---

[30] "AdMob by Google," *Google*, last accessed on August 15 2018, available at https://www.google.com/admob/
[31] "Hear form our happy customers," *Google,* last accessed on August 15 2018, available at
https://adwords.google.com/home/resources/success-stories/
[32] "Websites using Google Adsense," *BuiltWith,* last accessed on August 15 2018, available at
https://trends.builtwith.com/websitelist/Google-Adsense
[33] Google Analytics usage statistics," *BuiltWith,* April 2018, available at https://trends.builtwith.com/analytics/Google-Analytics
[34] Garett Sloane, "Google to retire Doubleclick and AdWords names in a rebrand of its as business," *Ad Age,* available at
http://adage.com/article/digital/google-waves-goodbye-doubleclick-ad-business-evolves/314046/

32.   Together, these tools collect information about user activities on websites and in apps, such as content visited, and ads clicked. They work in the background—largely unnoticeable by users. Figure 7 shows some of these key tools, with arrows indicating data collected from users and ads served to users.

Figure 7: Google products aimed at publishers and advertisers[35]
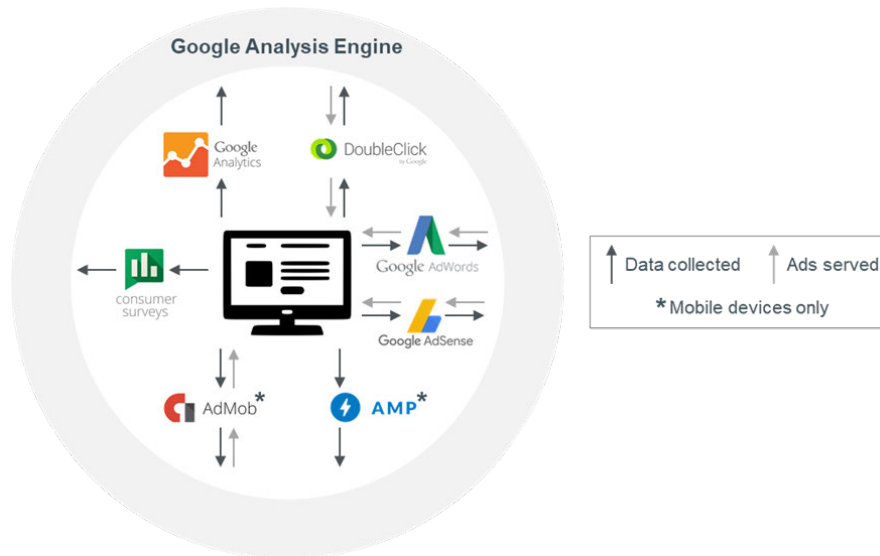
33.   The information collected by such tools includes a non-personal identifier that Google can use to send targeted advertisements without identifying the unique individual's personal information. These identifiers can be device- or session-specific, as well as permanent or semi-permanent. Table 1 lists a set of such identifiers. To provide users greater anonymity during information collection for ad targeting, Google has recently shifted towards using semi-permanent device unique identifiers (e.g. GAIDs).[36] Further sections go in detail about how these tools collect user data and the use of such identifiers during the data collection process.

Table 1: Identifiers passed to Google

Identifier	Type	Description
GAID/IDFA	Semi-Permanent	Alphanumeric string for Android / iOS devices to allow targeted mobile ads. Resettable by users.
Client ID	Semi-Permanent	ID created the first time a cookie is stored on the browser. Used to link browsing sessions together. Resets when browser cookies are cleared.
IP address	Semi-Permanent	A unique string of number that identifies the network through which a device is accessing the Internet.

---

[35] "Our products," *Google,* last accessed on August 15 2018, available at https://www.google.com/about/products/
[36] "Best practices for unique identifiers," *Google,* last accessed on August 15 2018, available at https://developer.android.com/training/articles/user-data-ids

Android device ID	Semi-Permanent	Randomly generated number when a device is first booted up. Used to identify the device. It is in the process of being phased out of advertising. Resets with a factory reset of a device.
Google Services Framework (GSF)	Semi-Permanent	Randomly assigned number when a user first logs into Google services on a device. Used to identify a unique device. Resets with a factory reset of a device.
IEMI / MEID	Permanent	Identifier used in mobile communication standards. Unique for each mobile phone.
MAC address	Permanent	Unique 12-character identifier for a piece of hardware (e.g. router).
Serial number	Permanent	Alphanumeric string used to identify a device.

A.   Google Analytics and DoubleClick

34.   DoubleClick and Google Analytics (GA) are Google's leading products in user behavior tracking and webpage traffic analyses on desktop and mobile devices. GA is used by ~75% of the top 100,000 most visited websites.[37] DoubleClick cookies are associated with more than 1.6 million websites.[38]

35.   GA uses short pieces of tracking code (called "page tags") embedded in a website's HTML code.[39] After a webpage loads per a user's request, the GA code calls an "analytics.js" file residing on Google's servers. This program transfers a "default" snapshot of user data at that moment, which includes visited webpage address, page title, browser information, current location (derived from IP address), and user language settings. GA scripts use cookies to track user behavior.

36.   GA script, the first time when it's run, generates and stores a browser-specific cookie on the user's computer. This cookie has a unique client identifier or Client ID (see Table 1 for details).[40] Google uses the unique identifier to link previously stored cookies that capture a user's activity on a particular domain as long as the cookie does not expire, or the user does not clear the cookies cached on their browser.[41]

37.   While a GA cookie is specific to the particular domain of the website that user visits (called a "1st-party cookie"), a DoubleClick cookie is typically associated with a common 3rd-party domain (such as

---

[37] Google Analytics usage statistics," *BuiltWith,* April 2018, available at https://trends.builtwith.com/analytics/Google-Analytics
[38] "DoubleClick market share," *Datanyze,* last accessed on August 15 2018, available at https://www.datanyze.com/market-share/ad-exchanges/doubleclick-market-share
[39] GA or other tags can also be implemented through Google Tag Manage (GTM) without changing the functionality of the page tag
[40] "Cookies and user identification," *Google*, last accessed on August 15 2018, available at https://developers.google.com/analytics/devguides/collection/analyticsjs/cookies-user-id
[41] "Cookies and user identification," *Google*, last accessed on August 15 2018, available at https://developers.google.com/analytics/devguides/collection/analyticsjs/cookies-user-id

doubleclick.net). Google uses such cookies to track user interaction across multiple 3rd-party websites.[42] When a user interacts with an advertisement on a website, DoubleClick's conversion tracking tools (e.g. Floodlight) places cookies on a user's computer and generates a unique client ID.[43] Thereafter, if the user visits the advertised website, the stored cookie information gets accessed by the DoubleClick server, thereby recording the visit as a valid conversion.

B.   AdSense, AdWords and AdMob

38.   AdSense and AdWords are Google tools that serve ads on websites and in Google Search results, respectively. More than 15 million websites have AdSense installed to display sponsored ads.[44] Likewise, more than 2 million websites and apps that make up the Google Display Network (GDN) and reach over 90% of Internet users[45] display AdWords ads.

39.   AdSense collects information about whether an ad was displayed on the publisher's webpage. It also collects how the user interacted with the ad, such as clicking an ad or tracking the curser movement over an ad.[46] AdWords enables advertisers to serve search ads on Google Search, display ads on publisher pages, and overlay ads on YouTube videos. To track user click-through and conversion rates, AdWords ads place a cookie on users' browsers to identify the same user if they later visit the advertiser's website or complete a purchase.[47]

40.   While AdSense and AdWords collect data on mobile devices as well, their ability to get user information on mobile devices is limited since mobile apps do not share cookie data between them, an isolation technique known as 'sandboxing,'[48] which makes it hard for advertisers to track user behavior across mobile apps.

41.   To address this issue, Google and other companies use mobile "ad libraries" (such as AdMob) that are integrated into the apps by their developers for serving ads in mobile apps. These libraries compile and run with the apps and send to Google data that is specific to the app to which they belong, including GPS locations, device make, and device model when apps have the appropriate permissions. As observed through the data

---

[42] "DoubleClick search help," *Google,* last accessed on August 15 2018, available at
https://support.google.com/ds/answer/7298761?hl=en
[43] "DoubleClick search help," *Google,* last accessed on August 15 2018, available at
https://support.google.com/ds/answer/2903014?hl=en&ref_topic=6054260
[44] "Websites using Google Adsense," *BuiltWith,* last accessed on August 15 2018, available at
https://trends.builtwith.com/websitelist/Google-Adsense
[45] "Google Ads Help," *Google,* last accessed on August 15 2018, available at https://support.google.com/google-ads/answer/2404191?hl=en
[46] "AdSense help, privacy and security," *Google,* last accessed on August 15 2018, available at
https://support.google.com/adsense/answer/9897?hl=en
[47] "Evaluating ad performance on the Search Network," *Google,* last accessed on August 15 2018, available at
https://support.google.com/adwords/answer/2404037?hl=en; "About conversion tracking," *Google,* last accessed on August 15 2018, available at https://support.google.com/adwords/answer/1722022?hl=en
[48] This approach is similar to desktops, where cookies are not shared between browsers.

traffic analyses (Figure 8), and confirmed through Google's own developer webpages,[49] such libraries can also send user-personal data, such as age and gender, to Google whenever app developers explicitly pass these values to the library.

Figure 8: Snapshot of information sent back to Google when an application is launched

C. Association of passively collected data with personal information

42. As discussed above, Google collects data through publisher and advertiser products and associate such data with a variety of semi-permanent, anonymous identifiers. Google however, has the ability to associate these IDs with a user's personal information. This is insinuated by the statements made in Google's privacy policy, excerpts of which are shown in Figure 9. The left text box clearly states that Google may associate data from advertising services and analytics tools with a user's personal information, depending upon the user's account settings. This arrangement is enabled by default, as shown in the right text box.

Figure 9: Google's privacy page for 3rd-party websites collection and association with personal information[50][51]

---
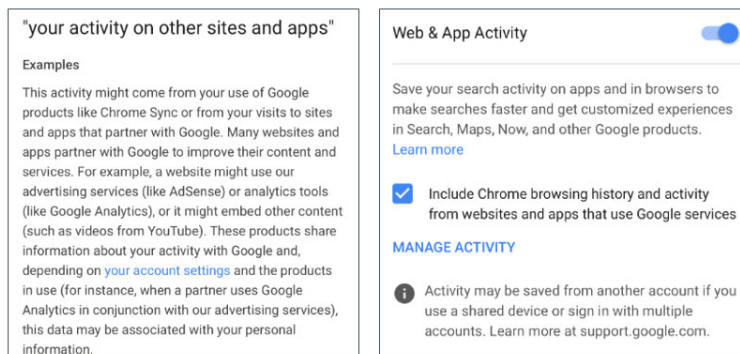
[49] "Google APIs for Android," *Google,* last accessed on August 15 2018, available at
https://developers.google.com/android/reference/com/google/android/gms/ads/doubleclick/PublisherAdRequest.Builder
[50] "Google privacy and terms," *Google,* last accessed on August 15 2018, available at
https://policies.google.com/privacy/example/your-activity-on-other-sites-and-apps
[51] "Google https://myaccount.google.com/activitycontrols

43.   Furthermore, an analysis of data traffic exchanged with Google servers (summarized below) identified two key examples (one on Android and the other in Chrome) that point to Google's ability to correlate anonymously collected data with users' personal information.

1)   Mobile advertising identifier may get de-anonymized through data sent to Google by Android

44.   Analyses of data traffic communicated between an Android phone and Google server domains suggest a possible way through which anonymous identifiers (GAID in this case) can get associated with a user's Google Account. Figure 10 describes this process through a series of three key steps.

45.   In step 1, a "checkin" data is sent to the URL *android.clients.google.com/checkin*. This particular communication provides an Android data sync to Google servers and contains Android log information (e.g. recovery log), kernel messages, crash dumps, and other device-related identifiers. A snapshot of a partially decoded checkin request sent to Google's server from Android is shown in Figure 10.

Figure 10: Device identifiers are sent together with account information in Android check in requests
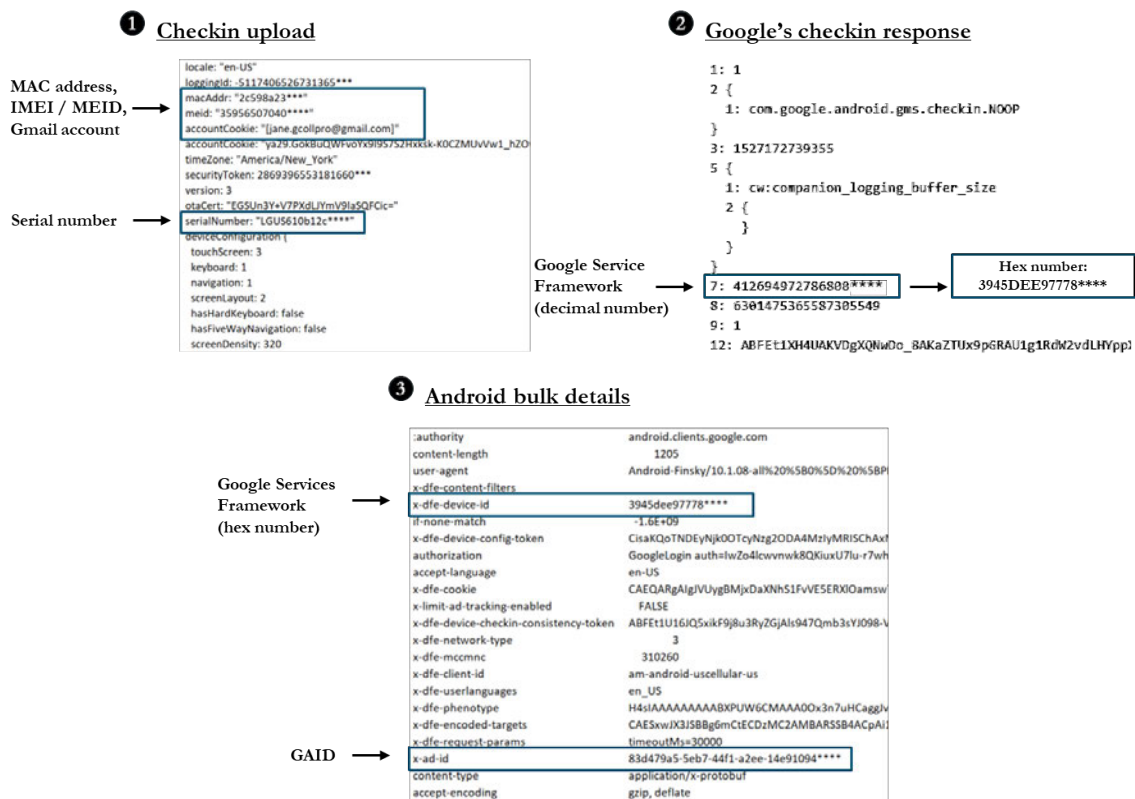
46.   As pointed out by the labeled boxes, through the checkin process, Android sends to Google a variety of important device-related permanent identifiers, including device MAC address, IMEI /MEID, and device

serial number. Moreover, these requests also contain the Android user's Gmail ID. The data present in checkin uploads enable Google to connect a user's personal information with Android device permanent identifiers.

47.   In step 2, the reply to the checkin request comes from the Google server. This message contains a Google services framework identifier (GSF ID)[52] that is similar to the actual "Android ID"[53] (see Table 1 for descriptions).

48.   Step 3 entails another instance of communication where the same GSF ID (from step 2) is sent to Google together with the GAID. Figure 10 shows one such data transmit to *android.clients.google.com/fdfe/bulkDetails ?au=1*.

49.   Through the above three data exchanges, Google receives the information needed to connect a GAID with permanent device identifiers as well as users' Google Account IDs.

50.   These intercepted data exchanges with Google servers from an Android phone show how Google can connect anonymized information collected on an Android mobile device via DoubleClick, Analytics or AdMob tools with the user's personal identity. During the 24-hour data collection from a stationary and dormant Android phone two instances of checkin communications with Google servers were observed. Additional analysis is needed, however, to determine if such information exchange occurs with a certain periodicity or if it is triggered by specific activities on the phones.

2)   DoubleClick cookie ID gets connected with user's personal information on Google Account

51.   The previous section explained how Google can de-anonymize user identity via the passive, anonymized data it collects from an Android mobile device. This section shows how such de-anonymization can also occur on a desktop/laptop device.

52.   Anonymized data on desktops/laptops is collected via cookie-based identifiers (e.g. Cookie ID), which are typically generated by Google's ad and publisher products (e.g. DoubleClick) and stored on a user's local mass storage. The experiment presented below assessed whether Google can connect such identifiers (and hence information associated with them) with a user's personal information. This experiment involved the following ordered steps:

1. Opened a new (no saved cookies, e.g. Private or Incognito) browser session (Chrome or other),

---

[52] "Difference between Android ID and device ID," *Stack Exchange,* Dec. 2016, available at
https://android.stackexchange.com/questions/162448/difference-between-android-id-and-device-id
[53] Patrick Ahlbrecht, "What's the difference between the GSF ID and the Android ID," *Onyxbits,* March 2016, available at
https://blog.onyxbits.de/whats-the-difference-between-the-gsf-id-and-the-android-id-208/

2. Visited a 3rd-party website that used Google's DoubleClick ad network,

3. Visited the website of a widely used Google service (Gmail in this case),

4. Signed in to Gmail.

53.   After completion of step 1 and 2, as part of the page load process, the DoubleClick server received a request when the user first visited the 3rd-party website. This request was part of a series of requests comprising the DoubleClick initialization process started by the publisher website, which resulted in the Chrome browser setting a cookie for the DoubleClick domain. This cookie stayed on user's computer until it expired or until the user manually cleared cookies via the browser settings.

54.   Thereafter, in step 3, when the user visited Gmail, they are prompted to log in with their Google credentials. Google manages identity using a "single sign on (SSO)" architecture, whereby credentials are supplied to an account service (signified by *accounts.google.com*) in exchange for an "authentication token," which can then be presented to other Google services to identify the users. In step 4, when a user accesses their Gmail account, they are effectively signing into their Google Account, which then provides Gmail with an authorization token to verify the user's identity. [54] This process is outlined by Figure 24 in Section IX.E in the Appendix.

55.   In the last step of this sign-on process, a request is sent to the DoubleClick domain. This request contains both the authentication token provided by Google and the tracking cookie set when the user visited the 3rd-party website in step 2 (this communication is shown in Figure 11). This allows Google to connect the user's Google credentials with a DoubleClick cookie ID. Therefore, if the users do not clear browser cookies regularly, their browsing information on 3rd-party webpages that use DoubleClick services could get associated with their personal information on Google Account.

Figure 11: Request to DoubleClick.net includes Google's authentication token and past cookies

---

[54] The advantage of the extra authentication step is that the user's browser can later use the same authentication token to confirm user identity on other Google services (due to this process a sign-on in any particular Google application enables an automatic sign-on all others in the same browser session).

22

56.   It has thus far been established that Google collects a wide variety of user data through its publisher and advertiser tools, without a direct knowledge of the user. While such data is collected with user-anonymous identifiers, Google has the ability to connect this collected information with a user's personal credentials stored in their Google Account.

57.   It's worth pointing out that Google's passive user data collection from 3rd-party webpages cannot be prevented using popular ad blocking tools,[55] as such tools are designed primarily to prevent the occurrence of advertisements while users browse through 3rd-party webpages.[56] The next section takes a closer look at the magnitude of such data collection.

V.   AMOUNT OF DATA COLLECTED DURING A MINIMAL USE OF GOOGLE PRODUCTS

58.   This section examines the details surrounding Google's data collection through its publisher and advertiser services. To understand such data collection, an experiment is designed which entailed a user going through her daily life using a mobile phone (akin to "day in the life" described before), while deliberately *avoiding* the use of any direct Google products (i.e. avoiding Search, Gmail, YouTube, Maps, etc.), except for the Chrome browser.

59.   To keep the experiment as realistic as possible, various consumer usage studies[57,58] were used to form a daily usage profile of a typical mobile phone user, thereafter, any direct interactions with Google's products were omitted from the profile. Section IX.F in the Appendix describes the websites and apps used in this experiment.

60.   The experiment was replicated on both Android and iOS devices and the HTTPS data sent to Google and Apple servers were monitored and analyzed using a similar method explained in previous sections. The results are summarized in Figure 12. During the 24-hour time period (which includes the night time stationary/dormant timeframe), the majority of calls from the Android phone were made to Google's location and publisher/advertisement service domains (e.g. DoubleClick, Analytics). Google collected user location in ~450 instances, which is ~1.4x times the experiment presented in Section III.C, which involved a stationary phone.

---

[55] "How many users block Google Analytics, measured in Google Analytics," *Quantable,* Dec. 2017, available at https://www.quantable.com/analytics/how-many-users-block-google-analytics/

[56] "Ad blocking: who blocks ads, why and how to win them back," *iab.,* 2016, available at https://www.iab.com/wp-content/uploads/2016/07/IAB-Ad-Blocking-2016-Who-Blocks-Ads-Why-and-How-to-Win-Them-Back.pdf

[57] The average person visited 88 webpages per day in 2010. "Nielsen provides topline U.S. web data for March 2010," *Nielsen,* April 2010, available at http://www.nielsen.com/us/en/insights/news/2010/nielsen-provides-topline-u-s-web-data-for-march-2010.html

[58] 55% of web traffic comes from mobile devices. Eric Enge, "Mobile vs desktop usage: mobile grows but desktop still a big player in 2017," *Stone Temple,* April 2017, available at https://www.stonetemple.com/mobile-vs-desktop-usage-mobile-grows-but-desktop-still-a-big-player-in-2017/

Figure 12: Information requests from mobile devices during a day of typical use
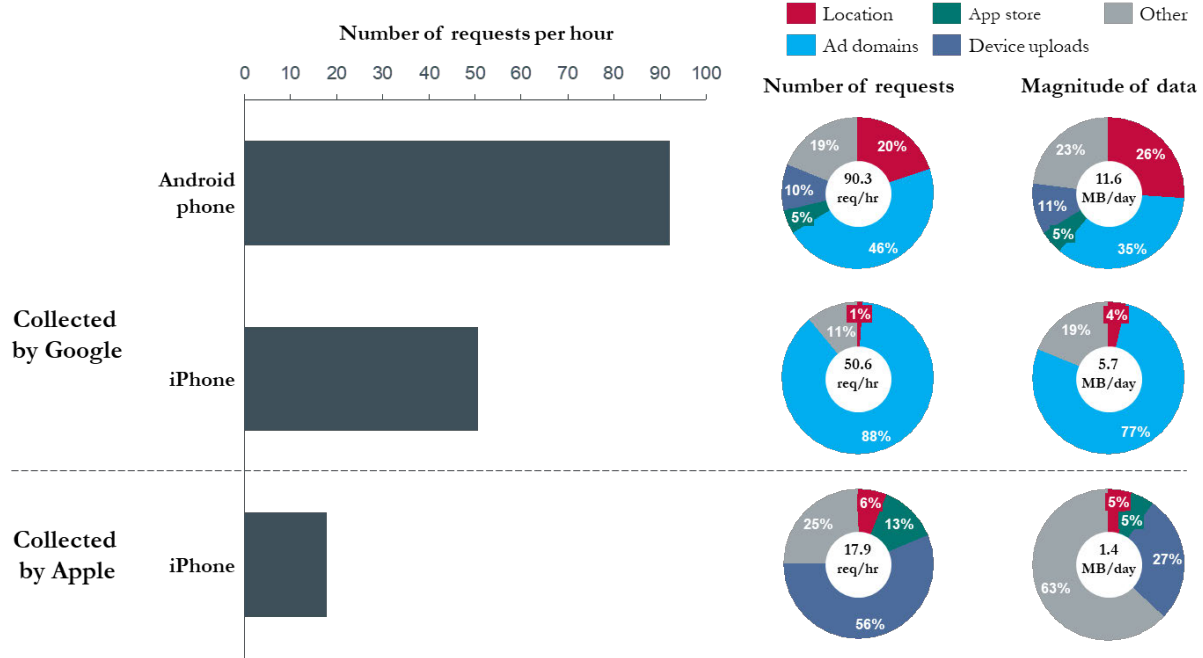
61.   Google servers communicated significantly lower number of times with an iPhone device compared to Android (45% less). However, the number of calls to Google's advertising domains were similar from both devices - an expected outcome since the usage of 3rd-party webpages and apps was similar on both devices. One notable difference was that the location data sent to Google from an iOS device is practically non-existent. In the absence of Android and Chrome platforms—or the use of any other Google product—Google becomes significantly limited in its ability to track the user location.

62.   The total number of calls to Apple servers from an iOS device was much lower, just 19% the number of calls to Google servers from an Android device. Moreover, there are no ad-related calls to Apple servers, which may stem from the fact that Apple's business model is not as dependent on advertising as Google's. Although Apple does obtain some user location data from iOS devices, the volume of data collected is much (16x) lower than what Google collects from Android.

63.   Magnitude wise, Android phones communicated 11.6 MB of data per day (~350 MB per month) with Google servers. On the other hand, the iPhone device communicated just half that amount. The amount of data particularly associated with Google's ad domains remained very similar across both the devices.

64.   The iPhone device communicated an order of magnitude less data to Apple servers than what the Android device exchanged with Google servers.

24

65.   Overall, even in the absence of user interaction with Google's most popular applications, a user of an Android phone and the Chrome browser still sends a significant amount of data to Google, the majority of which is associated with location and calls to ad server domains. Although an iPhone user is insulated from Google's location collection in this narrow experiment, Google still captures a similar amount of ad-related data.

66.   The next section describes the data collected by Google's popular applications, such as Gmail, YouTube, Maps, and Search.

VI.   DATA COLLECTED FROM GOOGLE'S KEY POPULAR APPLICATIONS AIMED AT INDIVIDUALS

67.   Google has dozens of constantly evolving products and services (a list is available in Table 4 in Section IX.B of the Appendix). These products are often accessed through—or associated with—a Google Account, which enables Google to directly link user activity details from its application-oriented products and services to a user profile. In addition to product usage data, Google also collects device-related identifiers and location data when Google's products and services are accessed.[59]

68.   Some of Google's applications (e.g. YouTube, Search, Gmail, and Maps) are central to the basic tasks that many users conduct daily through their desktop or mobile devices. Table 2 describes the reach of these key products. This section explains how each of these prominent applications collect user information.

Table 2: Worldwide reach of Google's top application products

Product	Active users
Search	Greater than 1B monthly active users, 90.6% search engine market share[60]
YouTube	Greater than 1.8 billion logged-in monthly active users[61]
Maps	Greater than 1 billion monthly active users[62]
Gmail	1.2 billion registered users[63]

---

[59] "Google privacy and terms," *Google,* last accessed on August 15 2018, available at https://policies.google.com/privacy
[60] "Search engine market share worldwide," *StatCounter Global Stats,* April 2018, available at http://gs.statcounter.com/search-engine-market-share#monthly-201704-201804
[61] Devindra Hardawar, "YouTube gets 1.8 billion logged-in viewers monthly," *Engadget,* May 3, 2018, available at https://www.engadget.com/2018/05/03/youtube-1-8-billion-viewers/
[62] Google 10K filings with the SEC, 2017, available at https://abc.xyz/investor/pdf/20171231_alphabet_10K.pdf
[63] Motek Moyen, "Gmail is very popular but Google still won't fix a security vulnerability," *Seeking Alpha,* July 17, 2017, available at https://seekingalpha.com/article/4088241-gmail-popular-google-still-fix-security-vulnerability

A.   Search

69.   Google Search is the most popular web search engine in the world,[64] with over 11 billion search queries per month in the United States alone.[65] In addition to serving ranked webpage results in response to users' general queries, Google operates other search-based tools, such as Google Finance, Flights, News, Scholar, Patents, Books, Images, Videos, and Hotels. Google uses its search products to collect data related to search queries, browsing history, and ad-click/purchase activity. For example, Google Finance collects information on the type of stocks users may be tracking, whereas Google Flights tracks users' travel bookings and search requests.

70.   Whenever Search is used, Google collects location data via various means of assessing locations on mobile or desktop devices, as discussed in previous sections. Google records all search activity a user conducts and links it back to their Google Account if the user is logged in. Figure 13 shows an example of information collected by Google about a user's keyword search and page visit.

Figure 13: An example search data collection taken from user's My Activity page
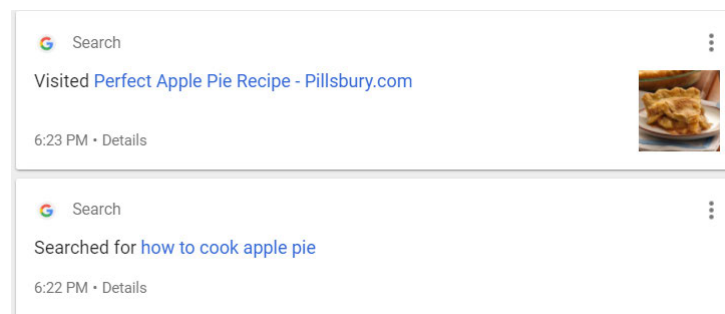
71.   In addition to being the default search engine on Chrome and Google devices, Google Search is also the default option on other 3rd-party browsers and applications through various distribution agreements. For example, Google recently became the default search engine on Mozilla's Firefox browser[66] in key geographic locations (including US and Canada), a position owned by Yahoo previously. Similarly, Apple switched from

---

[64] "Search engine market share worldwide," *StatCounter Global Stats,* April 2018, available at http://gs.statcounter.com/search-engine-market-share#monthly-201704-201804

[65] "Number of explicit core search queries powered by search engines in the United States as of January 2018 (in billions)," *Statista,* Feb. 2018, available at https://www.statista.com/statistics/265796/us-search-engines-ranked-by-number-of-core-searches/

[66] Denelle Dixon, "Firefox features Google as default search provider in the U.S., Canada, Hong Kong and Taiwan," *The Mozilla Blog,* Nov. 14, 2017, available at https://blog.mozilla.org/blog/2017/11/14/firefox-features-google-as-default-search-provider-in-the-u-s-canada-hong-kong-and-taiwan/

Microsoft's Bing to Google for Siri web search results on iOS and Mac devices.[67] Google has similar agreements in place with OEMs,[68] which helps reach mobile customers.

B.   YouTube

72.   YouTube provides users a platform for uploading and viewing video content. It has more than 180 million users in the USA alone and has the distinction of being the second-most visited website in the US,[69] ranked only behind Google Search. Among online streaming media companies, YouTube has almost 80% market share in terms of monthly user visits (as shown in Figure 14). The amount of content uploaded and viewed on YouTube is substantial; ~400 hours of video are uploaded every minute[70] and ~1 billion hours of video are watched daily on the YouTube platform.[71]

Figure 14: Comparison of leading multimedia websites monthly visits in the United States[72]
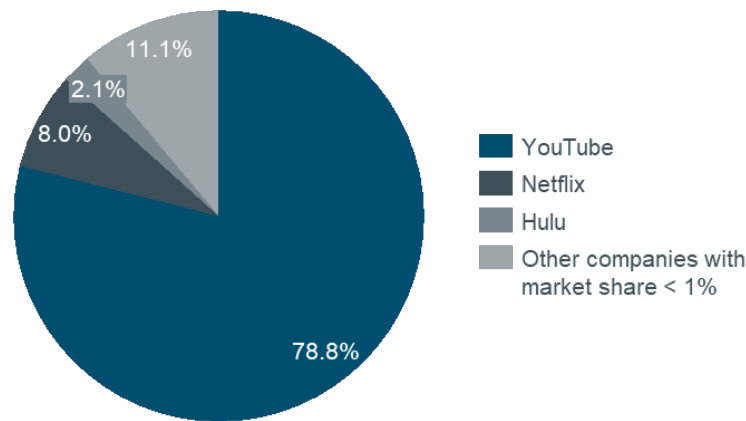
73.   YouTube can be accessed by users via desktops (web browser), mobile devices (app and/or web browser), and Google Home (through a paid subscription service called YouTube Red). Google collects and stores search history, watch history, playlists, subscriptions, and comments on videos. All this information is marked with a date and time stamp of when the activity took place.

---

[67] Matthew Panzarino, "Apple switches from Bing to Google for Siri web search results on iOS and Spotlight on Mac," Sept. 25, 2017, available at https://techcrunch.com/2017/09/25/apple-switches-from-bing-to-google-for-siri-web-search-results-on-ios-and-spotlight-on-mac/

[68] "Google's Android mobile application distribution agreement with OEMs leaked, reveals lots of strict conditions," *Microsoft and Technology News,* Feb. 13, 2014, available at https://mspoweruser.com/mobile-application-distribution-agreement/

[69] "Top Sites in United States," *Alexa,* available at https://www.alexa.com/topsites/countries/US

[70] "Hours of video uploaded to YouTube every minute as of July 2015," *Statista,* July 2015, available at https://www.statista.com/statistics/259477/hours-of-video-uploaded-to-youtube-every-minute/

[71] Darrell Etherington, "People now watch 1 billion hours of YouTube per day," *TeachCrunch*, Feb. 28, 2017, available at https://techcrunch.com/2017/02/28/people-now-watch-1-billion-hours-of-youtube-per-day/

[72] "Leading multimedia websites in the United States in November 2016, based on market share of visits," *Statista,* Dec. 2016, available at https://www.statista.com/statistics/266201/us-market-share-of-leading-internet-video-portals/

74.   If a user is signs into their Google Account on any Google application inside a browser (e.g. Chrome, Firefox, Safari), Google recognizes the user's identity, even if the video is accessed through a non-Google website (e.g. YouTube videos played through CNN.com). This feature allows Google to track a user's YouTube usage across multiple 3rd-party platforms. Figure 15 shows an example of YouTube data collected.

Figure 15: An example of YouTube data collection from My Activity
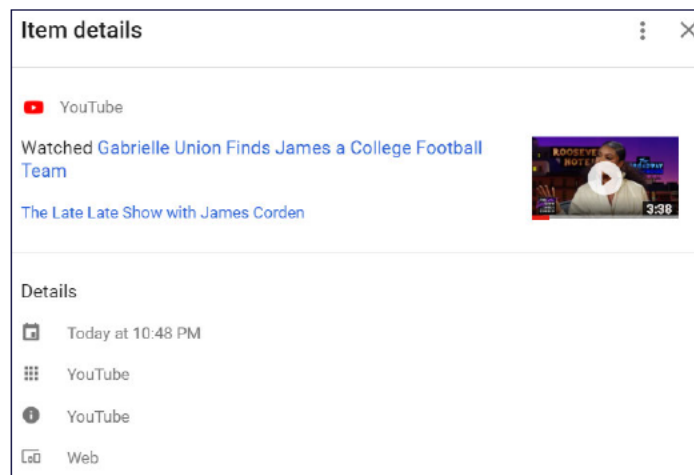
75.   Google also offers a separate YouTube product for children, known as YouTube Kids, which is intended as a "family friendly" version of YouTube with parental control features and video filters. Google collects information from YouTube Kids, including device type, operating system, unique device identifiers, log information, and details of how the service was used. Google then uses this information to deliver limited advertisements that are non-clickable, and which have restrictions on format, time length, and site-served.[73]

C.   Maps

76.   Maps is Google's flagship navigation app. Google Maps can ascertain user's travel routes, speed, and places that a user visits frequently (e.g. home, work, restaurants, and businesses). This information provides Google with a window into a user's interests (e.g. food and shopping preferences), movement, and behavior.

77.   Maps uses IP address, GPS, cell signal, and Wi-Fi access point data to calculate a device's location. The latter two are collected from the device through which Maps is used and sent to Google for location assessment through its Location API. This API provides rich details about a user, including geographic coordinates, whether the user is stationary or moving, speed, and probabilistic determination of user's mode of transport (e.g. bike, car, train, etc.).

---

[73] "Advertising on YouTube Kids," *Google*, last accessed on August 15 2018, available at https://support.google.com/youtube/answer/6168681?hl=en

78.   Maps stores a historical timeline of places visited by a user signed in to Maps using their Google account. Figure 16 shows an example of such a user's timeline.[74] The red dots indicate location coordinates captured by Maps while the user is on the move; the blue connecting lines are Maps projection of the actual route the user took.

Figure 16: Example Google Maps "Timeline" from an actual user
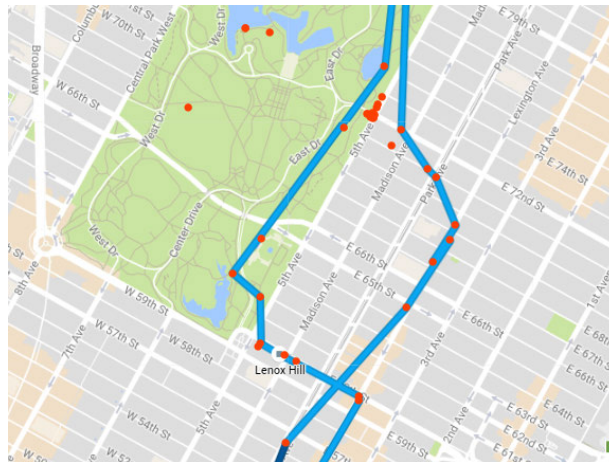
79.   The accuracy of location information captured by navigation applications enables Google to not only target ad audiences, but also helps deliver ads to users as they approach stores.[75] In addition, Google Maps uses this information to generate real-time traffic updates.[76]

D.   Gmail

80.   Gmail stores all messages (sent/received), sender name, email address, and date/time of messages sent or received. Since Gmail acts as a central mail repository for many people, it can ascertain their interests by scanning email content, identifying merchant addresses through their promotional emails or sales receipts sent to emails, and learn about a user's plans (e.g. dinner reservations, doctor's appointments,). Since users may use their Gmail ID for other 3rd-party platforms (e.g. Facebook, LinkedIn), Gmail can scan any content that comes from them in the form of an email (e.g. notifications, messages).

81.   From its inception in 2004 until at least late 2017, Google may have scanned the contents of Gmail emails to improve ad targeting and search results, as well as filter spam. In the summer of 2016, Google went a step further and changed its privacy policy to enable it to combine formerly anonymous web-browsing data

---

[74] "My Activity," *Google*, available at https://myactivity.google.com/myactivity
[75] "The Home Depot earns 8X in-store ROI with mobile display ads," *Google,* Sept. 2016, available at https://www.thinkwithgoogle.com/intl/en-aunz/advertising-channels/mobile/home-depot-roi-mobile-display-ads/
[76] "Google Map's real-time traffic layer…," *Spatial Unlimited,* March 2011, available at https://shreerangpatwardhan.blogspot.com/2011/03/google-maps-real-time-traffic-layer.html

of its subsidiary DoubleClick (which serves customized ads across the Internet) with the personally-identifying data Google has through its other products, including Gmail.[77] The result was that "…the DoubleClick ads that follow people around on the web may now be customized to them based on keywords they used in their Gmail. It also meant that Google could now build a complete portrait of a user by name, based on everything they write in email, every website they visit, and the searches they conduct."[78]

82.   Toward the end of 2017, Google announced it would discontinue the practice of Gmail message-based personalization of ads.[79] Recently, however, Google clarified that it is still scanning Gmail messages for some purposes.[80]

VII.   PRODUCTS WITH HIGH FUTURE POTENTIAL FOR DATA AGGREGATION

83.   Google has additional products that show future potential for market adoption and data collection, including AMP, Photos, Chromebook, Assistant, and Pay. Additionally, Google is able to use third party data vendors to collect user information. The following sections describe these in greater detail.

84.   There are other Google applications that may not be widely used, however for completeness, data collection through them is presented in Section VIII.B of the Appendix.

A.   Accelerated Mobile Pages (AMP)

85.   Accelerated Mobile Pages (AMP) is an open-source initiative spearheaded by Google to enable quicker load times for websites and ads. AMP converts conventional HTML and JavaScript code into a more simplified version developed by Google[81] and caches the AMP-validated webpages in Google's network of servers for faster access.[82] AMP delivers page links through Google search results, as well as 3rd-party platforms, such as LinkedIn and Twitter. As the AMP page reports: "AMP's ecosystem includes 25 million domains, 100+ technology providers and leading platforms, that span the areas of publishing, advertising, e-commerce, local and small businesses, and more!"[83]

---

[77] Julia Angwin, "Google has quietly dropped ban on personally identifiable web tracking," *ProPublica,* Oct. 21, 2016, available at
https://www.propublica.org/article/google-has-quietly-dropped-ban-on-personally-identifiable-web-tracking
[78] Suzanne Monyak, "Google changed a major privacy policy four months ago, and no one really noticed," *Slate,* Oct. 21, 2016, available at
http://www.slate.com/blogs/future_tense/2016/10/21/google_changed_a_major_privacy_policy_and_no_one_really_noticed.html
[79] Mark Bergen, "Google will stop reading your emails for Gmail ads," *Bloomberg,* June 23, 2017, available at
https://www.bloomberg.com/news/articles/2017-06-23/google-will-stop-reading-your-emails-for-gmail-ads
[80] Ben Popken, "Google sells the future, powered by your personal data," *NBC News,* May 10, 2018, available at
https://www.nbcnews.com/tech/tech-news/google-sells-future-powered-your-personal-data-n870501
[81] "AMP HTML specification," *AMP,* last accessed on August 15 2018, available at
https://www.ampproject.org/docs/fundamentals/spec
[82] "Load AMP pages quickly with Google AMP Cache," *Google,* last accessed on August 15 2018, available at
https://developers.google.com/amp/cache
[83] "An open source effort to improve the content ecosystem for everyone," *AMP*, last accessed on August 15 2018, available at
https://www.ampproject.org/learn/overview

86.   Figure 17a describes the steps leading to the delivery of an AMP page accessed via Google Search. Please note that the provider of content through AMP does not need to provide their own a cache server, as this is something that Google provides for securing optimal delivery speeds to users. Since the AMP cache is hosted on Google servers, when an AMP link is clicked through Google Search, the domain address shows up from a Google.com domain rather than from a publisher's own domain. This is shown through snapshots taken from an example keyword search in Figure 17b.

Figure 17: Regular web page vs AMP page
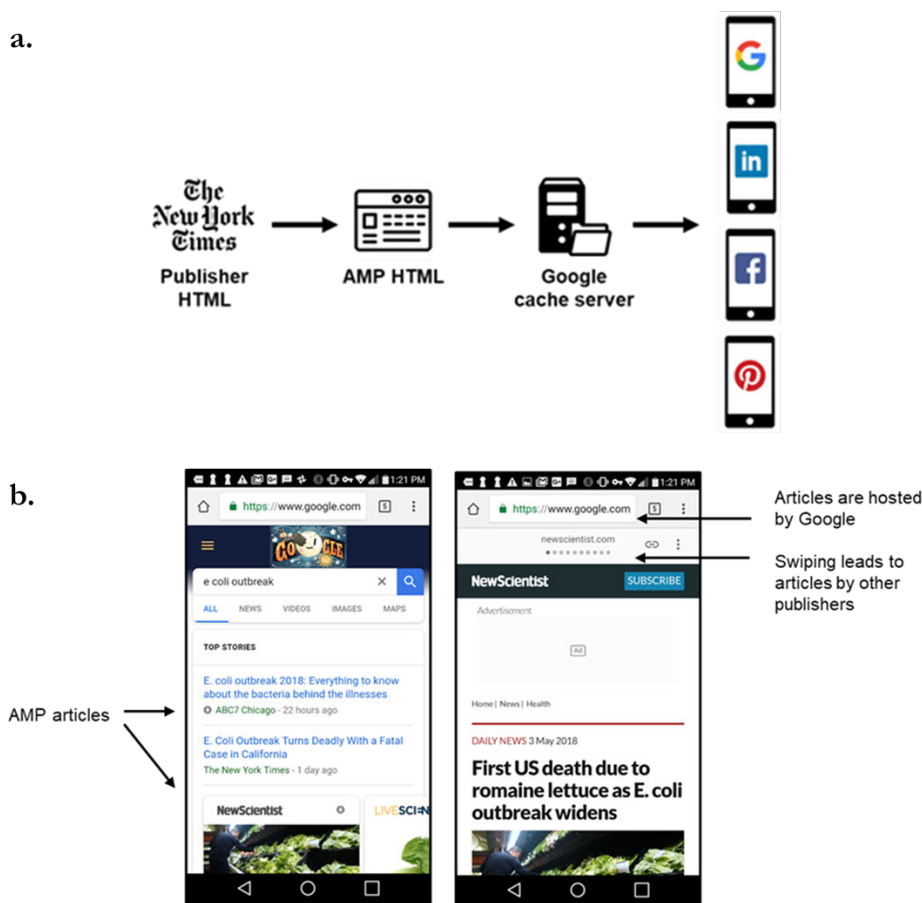
87.   Users can access content from multiple publishers whose articles appear in search results while navigating the AMP carousel, all while staying within the Google domain. In effect, the AMP cache operates as a content delivery network (CDN) owned and operated by Google.

88.   By creating an open-source tool, complete with a CDN, Google has attracted a large user base for serving mobile websites and advertisements that constitute a significant amount of information (e.g. the content itself, page views, ads served, and information on whom that content is being delivered). All of this information

31

is available to Google by virtue of it residing on Google's CDN servers, thereby providing Google far more data than it otherwise could access.

89.   AMP is highly user-centric, i.e. it delivers a much faster and improved browsing experience to users without the clutter of pop-ups and sidebars. Although AMP is a major shift in the way content is cached and delivered to users, Google's privacy policy associated with AMP is quite general.[84] In particular, Google is able to collect webpage usage information (e.g. server logs and IP address) from requests sent to AMP cache servers. Moreover, regular pages are converted into AMP via the use of AMP APIs.[85] Google can therefore access applications or websites ("API clients") and use any submitted information through the API in accordance with its general policies.[86]

90.   Like regular webpages, AMP webpages track usage data via Google Analytics and DoubleClick. In particular, they collect information on page data (e.g. domain, path, and page title), user data (e.g. client ID, time zone), browsing data (e.g. unique page view ID and referrer), browser info, and interaction and events data.[87] Although Google's modes of data collection have not changed with AMP, the *amount* of data collected has increased since visitors are spending 35% more time on web content that loads with Google AMP versus standard mobile pages.[88]

B.   Google Assistant

91.   Google Assistant is a virtual personal assistant accessed through mobile phones and smart devices. It is a popular virtual assistant, alongside Apple's Siri, Amazon's Alexa, and Microsoft's Cortana.[89] Google Assistant is accessed through the home button of mobile devices with Android 6.0 or higher. It can also be accessed through a dedicated app on iOS devices[90], as well as smart speakers, such as Google Home. Google Assistant performs numerous functions, such as sending texts, looking up emails, controlling music, searching photos, getting answers to questions about the weather or traffic, and controlling smart home devices.[91]

92.   Google collects all Google Assistant queries, whether audio or typed. It also collects the location where the query occurred. Figure 18 shows the content of a query stored by Google. In addition to its use on Google's

---

[84] "AMP on Google privacy and terms," *Google,* last accessed on August 15 2018, available at
https://developers.google.com/amp/cache/policies
[85] "Link to AMP content," *Google,* last accessed on August 15 2018, available at https://developers.google.com/amp/cache/use-amp-url
[86] "Google APIs terms of service," *Google*, last accessed on August 15 2018, available at https://developers.google.com/terms
[87] "Tracking accelerated mobile pages (AMP)," *Google,* last accessed on August 15 2018, available at
https://support.google.com/analytics/answer/6343176?hl=en&ref_topic=7378717
[88] John Saroff, "The new speed of mobile engagement," *Chartbeat,* June 5, 2017, available at
http://blog.chartbeat.com/2017/06/05/the-new-speed-of-mobile-engagement
[89] Tripp Mickle, "'I'm not sure I understand' – how Apple's Siri lost her mojo," *The Wall Street Journal,* June 7, 2017, available at
https://www.wsj.com/articles/apples-siri-once-an-original-now-struggles-to-be-heard-above-the-crowd-1496849095
[90] "Google Assistant," *Google,* last accessed on August 15 2018, available at https://assistant.google.com/platforms/phones/
[91] "Google Assistant," *Google,* last accessed on August 15 2018, available at https://assistant.google.com/platforms/phones/

Home speakers, Google Assistant is enabled on various other speakers produced by 3rd-parties (e.g. Bose wireless headphones). Overall, Google Assistant is available on more than 400 million devices.[92] Google can collect data via all these devices since Assistant queries go through Google's servers.

Figure 18: Example of detail collected from Google Assistant query
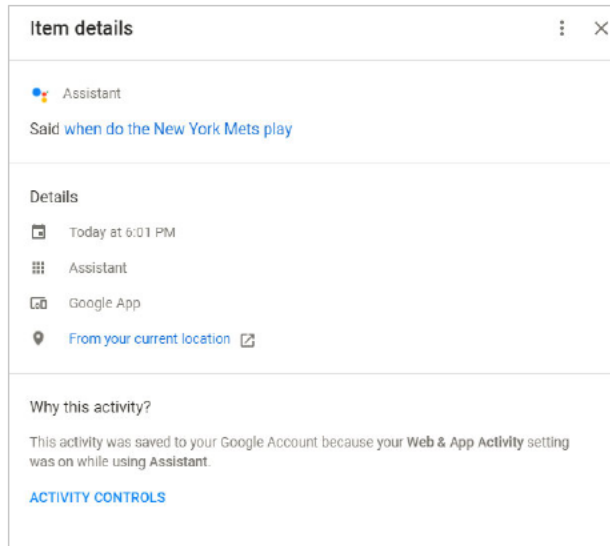
C.   Photos

93.   Google Photos is used by more than 500 million people globally and stores more than 1.2 billion photos and videos every day.[93] Google records the time and GPS coordinates for every photo taken. Google uploads images to the Google cloud and conducts image analysis to identify a broad set of objects, such as modes of transportation, animals, logos, landmarks, text, and faces.[94] Google's face detection capabilities even enable the detection of emotional states associated with faces in photos uploaded and stored in their cloud.[95]

94.   Google Photos conducts this image analysis by default when the product is used, but will not distinguish between individual people unless the user gives the app permission.[96] If a user provides permission for Google to group similar faces together, Google identifies different people using facial recognition

---

[92] Scott Huffman, "New devices and more: what's in store for the Google Assistant this year." *Google,* Jan. 9, 2018, available at https://www.blog.google/products/assistant/new-devices-more-google-assistant-ces-2018
[93] Anil Sabharwal, "500 million people using Google Photos, and three new ways to share," *Google,* May 17, 2017, available at https://blog.google/products/photos/google-photos-500-million-new-sharing/
[94] "Cloud vision API," *Google,* last accessed on August 15 2018, available at https://cloud.google.com/vision/
[95] "Cloud vision API," *Google,* last accessed on August 15 2018, available at https://cloud.google.com/vision/
[96] "Find people, things, and places in your photos," *Google,* last accessed on August 15 2018, available at https://support.google.com/photos/answer/6128838?co=GENIE.Platform%3DAndroid&hl=en

technology and enables users to share photos based on its "face grouping" technology.[97,98] Examples of Google's image classification capabilities with and without face grouping permission from the user are shown in Figure 19. Google uses Photos to assemble a vast trove of identifying facial information, which has become the subject of recent lawsuits[99] by certain states.

Figure 19: Example image recognition in Google Photos
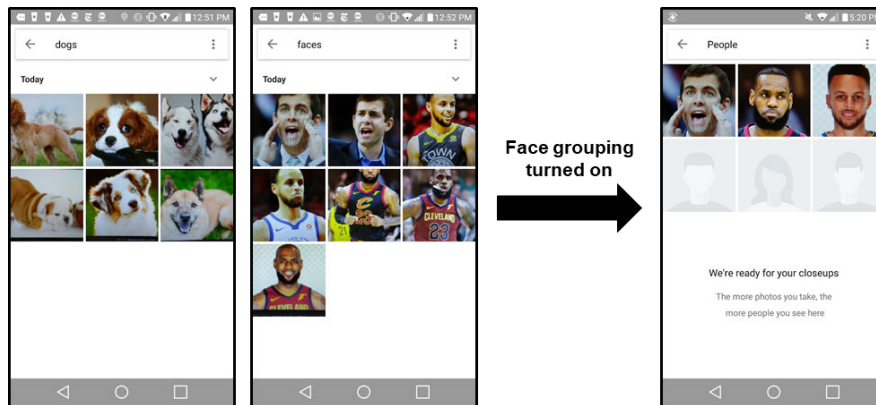
D.   Chromebook

95.   Chromebook is Google's tablet computer running on the Chrome operating system (Chrome OS) which allows users to access applications on the cloud. While Chromebook holds a very small fraction of the PC market, it's growing rapidly, especially in computing devices for the K-12 category, where it held 59.8% of the market in Q2 2017.[100] Since Chromebook is accessed through a Google Account, a user is always signed on to all of Google's applications while accessing them on a Chromebook device. Chromebook's data collection is similar to the Google Chrome browser, which is covered in section II.A. Chromebooks also allow cookies from Google and 3rd-party domains to track user activity, similar to any other notebook or PC device.

96.   Many K-12 schools use Chromebooks to access Google's products via its GSuite for Education service. Google states that data collected from such use is not used for targeted advertising.[101] Students are shown ads, however, if they use additional services (such as YouTube or Blogger) on Chromebooks provided through their educational institutions.

---

[97] Anil Sabharwal, "500 million people using Google Photos, and three new ways to share," *Google,* May 17, 2017, available at https://blog.google/products/photos/google-photos-500-million-new-sharing/
[98] "Share your Google Photos library with a partner," *Google*, last accessed on August 15 2018, available at https://support.google.com/photos/answer/7378858#filterbyface
[99] Amy Korte, "Federal court in Illinois rules biometric privacy lawsuit against Google can proceed," *Illinois Privacy,* March 8, 2017, available at https://www.illinoispolicy.org/federal-court-in-illinois-rules-biometric-privacy-lawsuit-against-google-can-proceed/
[100] "Mobile PC sales in to US K-12 education starting to slow as the market looking toward replacement cycles," *Future Source Consulting,* Dec. 6, 2017, available at https://www.futuresource-consulting.com/Press-Q3-2017-Mobile-PC-Sales-in-Education-1217.html
[101] "Chromebooks privacy and security," *Google,* last accessed on August 15 2018, available at https://drive.google.com/file/d/0B__OTXR_u3RbcFB3Y01xUVhaalU/view

E.   Google Pay

97.   Google Pay is a digital payments service that allows users to store credit card, bank account, and PayPal information to make payments in stores, on websites, or within apps using Google Chrome or a connected Android device.[102] Pay is the means by which Google collects verified user address and phone numbers, as these are associated with charge accounts. In addition to personal information, Pay also collects transaction information, such as date and amount of transaction, merchant location and description, type of payment used, descriptions of the items purchased, any photo that a user choose to associate with the transaction, names and email addresses of the seller and buyer, the user's description of the reason for transaction, and any offers associated with the transaction.[103] Google treats this information as personal information under its general privacy policy. It therefore can use this information across its products and services for enriched advertising.[104] Google's privacy settings allow for such a use of collected data by default.[105]

F.   User data collected from 3rd-party data vendors

98.   Google collects 3rd-party data in addition to information they collect directly from their services and applications. For example, in 2014 Google announced that it would begin tracking sales in brick-and-mortar stores by buying credit and debit card transaction data. Such data covered 70% of all credit and debit transactions in the US.[106] It contained the name of the individual, as well as the time, location, and amount of their purchase.[107]

99.   3rd-party data is also used to support Google Pay, including verification services, information arising from Google Pay transactions at merchant locations, payment methods, identity of card issuers, information regarding access to balances in the Google payment account, carrier and operator billing information, and consumer reports.[108] For sellers, Google may obtain information from credit bureaus or business information services.

100.   Although the 3rd-party user information that Google currently receives is limited in scope, it has already attracted the attention of governmental authorities. For example, the FTC announced an injunction against

---

[102] "Google Pay," *Google,* last accessed on August 15 2018, available at https://pay.google.com/about/
[103] "Google Payments privacy notice," *Google*, Dec. 14, 2017, available at https://payments.google.com/payments/apis-secure/u/0/get_legal_document?ldo=0&ldt=privacynotice&ldl=en
[104] "Google Payments privacy notice," *Google*, Dec. 14, 2017, available at https://payments.google.com/payments/apis-secure/u/0/get_legal_document?ldo=0&ldt=privacynotice&ldl=en
[105] "Google payments center," *Google,* available at https://payments.google.com/payments/home?page=privacySettings#privacySettings:
[106] "Google plans to track credit card spending," *BBC,* May 26, 2017, available at http://www.bbc.com/news/technology-40027706
[107] Elizabeth Dwoskin and Craig Timberg, "Google now knows when its users go to the store and buy stuff," *The Washington Post,* May 23, 2017, available at https://www.washingtonpost.com/news/the-switch/wp/2017/05/23/google-now-knows-when-you-are-at-a-cash-register-and-how-much-you-are-spending/?utm_term=.281715f8e215
[108] "Google Payments privacy notice," *Google*, Dec. 14, 2017, available at https://payments.google.com/payments/apis-secure/u/0/get_legal_document?ldo=0&ldt=privacynotice&ldl=en

Google in July 2017 with respect to how Google's collection of consumer purchasing data infringes upon electronic privacy. [109] The injunction challenges Google's claim that they can protect consumer privacy throughout the process using their algorithm. Although further action has not yet occurred, the FTC injunction is an example of public concern with the amount of consumer data that Google collects.

VIII.   CONCLUSION

101.   Google counts a large percentage of the world's population as its direct customers, with multiple products leading their markets globally and many surpassing 1 billion monthly active users. These products are able to collect user data through a variety of techniques that may not be easily graspable by a general user. A major part of Google's data collection occurs while a user is not directly engaged with any of its products. The magnitude of such collection is significant, especially on Android mobile devices. And while such information is typically collected without identifying a unique user, Google distinctively possesses the ability to utilize data collected from other sources to de-anonymize such a collection.

---

[109] FTC Complaint, request for investigation, injunction, and other relief submitted by The Electronic Privacy Information Center, available at https://epic.org/privacy/ftc/google/EPIC-FTC-Google-Purchase-Tracking-Complaint.pdf

IX.   APPENDIX

A.   Characterization of active vs passive data collection from "day in the life" of a user

Table 3: Active and passive Google data collection

Number	Description	Active collection	Passive collection
1	Gets ready in the morning while listening to Google Play Music	• Music interests	• Morning location
2	Drops kids off at daycare before commuting to work		• Walked to a daycare location
3	Checks the news while commuting to work on the subway		• Traveling on the subway • News pages visited
4	Searches for cold medicine while on the subway	• Records search queries	• Traveling on the subway
5	Walks from subway to work		• Commute path to work address
6	Uses Maps to find a new lunch spot	• Destination entered into Maps	• Dining interests
7	Gets coffee from Starbucks using her Starbucks app		• Walks to a Starbucks • Opens Starbucks app
8	Schedules doctor's appointment, Google creates a Calendar event from the confirmation email		• Event details of the doctor appointment
9	Walks to Walgreens and purchases cold medicine using Google Pay	• Purchase details	• Walks to a Walgreens
10	Takes an Uber home from work		• Commute path to home address via car • Use of Uber app
11	Looks for hotels on Expedia for a weekend trip		• Webpage interaction via DoubleClick cookies & Google Analytics
12	Uses Google Home to play music for her kids	• Google Home search query	• Location of Google Home

13	Watches videos on YouTube	• YouTube activity

B.   List of Google products

Table 4: List of Google Products

Category	Products
1. Applications	**Watch, Listen and Play** YouTube, Google Play Music, Chromecast, Google Play Movies and TV
	Browser Chrome
	Search Search, Finance, Flights, News, Scholar, Patents, Books, Images, Videos, Hotels
	Navigation Maps, Waze
	Productivity tools Drive, Docs, Sheets, Slides, Forms
	Social & communications Gmail, Allo, Hangouts, Duo, Google+, Translate
	Storage and organization Photos, Contacts, Calendar, Keep
	Personal Assistant Google voice assistant
2. Operating systems	**Android** Phones, Wear, Auto
	Chrome Chromebook
3. Services	Fiber, DNS, Project Fi, Google pay
4. Devices	Home, Wi-Fi router, Chromecast, Nest, Daydream View

C.   Data collection from other prominent Google products

a)   Google Play Music and Play Movies and TV

38

102.   Google Play Music, Play Movies and TV are on-demand services that offer streaming of music, podcasts, TV shows, and movies. These services can be thought of as the Google equivalent of Apple iTunes. Like YouTube, these services collect information about user search, bought/rent/played content, information about users' geography (through IP address), and device information.

b)   Waze

103.   Waze got acquired by Google in 2013 and operates as a Google subsidiary. In contrast to Maps, Waze is a crowd-sourced app where user-supplied data (such as GPS location coordinates, travel times, traffic info, accidents, police monitoring, blocked roads, and construction) is analyzed to provide routing and real-time travel condition updates. In addition to location information collected through the mobile device, Waze collects information about use of its services from the device Waze is installed on, including mobile device name, operating system, web page visits, information viewed on app, app content use/created, and ads viewed and clicked.

104.   Waze works like a social network and provides users the ability to befriend other users and create an online community of local drivers.[110] Users can link their phone's contact list, Facebook, or Twitter accounts, which Waze then uses to match with friends on platforms who are also using Waze's service. Overall, Waze gives Google the ability to access more real-time user data, as well as information on acquaintances that may or may not be using a Google Account.

c)   Google Docs and Drive

105.   Google's productivity tools (Docs, Sheets, Slides, Forms, and Drive – which are part of the broader "G Suite" of products) are cloud-based applications used by both individuals and enterprises. Google's G Suite privacy policies[111] prohibit Google from scanning stored data for advertising purposes on enterprise versions. In contrast, the free versions of these tools are governed by Google's general privacy policy, so Google may access the information for ad targeting.

106.   After an individual registers for a Google Account, Google provides free storage space (currently 15GB) on Google Drive to share across products including Gmail, Photos, and Docs. Google's Terms of Service indicate that Google retains the license to use the stored data in variety of ways, including reproducing,

---

[110] J.D. Biersdorfer, "Getting social with Waze," *The New York Times,* Sept. 20, 2017, available at
https://www.nytimes.com/2017/09/20/technology/personaltech/getting-social-with-waze.html
[111] "Google Cloud help, privacy," *Google,* last accessed on August 15 2018, available at
https://support.google.com/googlecloud/answer/6056650?hl=en

modifying, communicating, and publishing.[112] Although all user data stored in Google Drive is encrypted, it's not a "zero-knowledge encryption"[113] since Google manages the data encryption key.

d)   Video chat and social messaging apps

107.   Google Hangouts is a communication platform, akin to Skype, and a part of Google's G Suite cloud-connected apps. Users can start and join video conferences or group conversations from the Hangout app available on Android and iOS, through a web browser, from the Hangouts desktop app or Chrome extension, and from other Google products (e.g. Gmail and Calendar).[114] Google stores details of these exchanges (including conference call and conversation time stamps), participant information, and message content. These details are available to users and can be downloaded via the Google Takeout tool.[115] Figure 20 shows some data recorded from a Google Hangouts conversation, including participant names, participant IDs, and the contents of the conversation.

Figure 20: Google Takeout recordings of a Google Hangouts Conversation
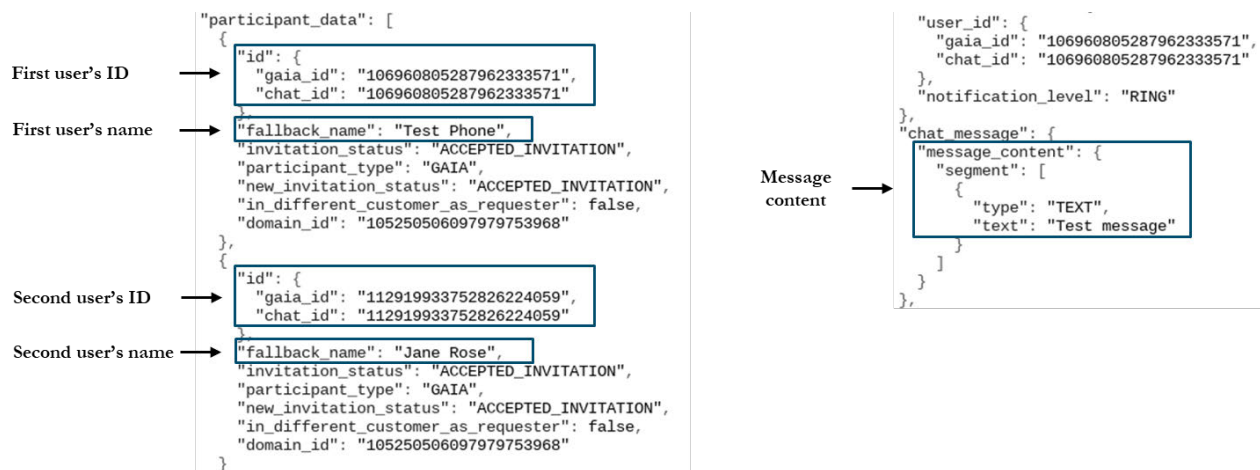
108.   In addition to the enterprise-focused Hangouts, Google also offers an instant messaging app called Allo, which is available for Android and iOS or through web browsers.[116] Google records and stores all messages communicated through Allo by default (unless the user invokes incognito mode).[117]

---

[112] "Google Drive terms of service," *Google,* last accessed on August 15 2018, available at https://www.google.com/drive/terms-of-service

[113] Fergus O'Sullivan, "What exactly is zero-knowledge in the cloud and how does it work?," *Cloudwards,* June 16, 2017, available at https://www.cloudwards.net/what-exactly-is-zero-knowledge-in-the-cloud-and-how-does-it-work

[114] "GSuite learning center," *Google,* last accessed on August 15 2018, available at https://gsuite.google.com/learning-center/products/hangouts/get-started/#!/

[115] "Download your data," *Google*, available at https://takeout.google.com/settings/takeout?pli=1

[116] Sean Keach, "Google Allo just got a major upgrade – but do we really need it?," *Trusted Reviews,* Aug. 16, 2017, available at http://www.trustedreviews.com/news/google-allo-3261336

[117] Russell Brandom, "Google backs off on previously announced Allo privacy feature," *The Verge,* Sept. 21, 2016, available at https://www.theverge.com/2016/9/21/12994362/allo-privacy-message-logs-google

109.   Google offers an app called Google Duo that is a dedicated mobile video chat app. It is available both on Android and iOS, but not on desktop/laptop computers. Users can call or video chat each other and even connect with users on the Android operating system who have not downloaded the app.[118] Once installed, Google Duo has access to a user's profile data, contacts, camera, microphone, Wi-Fi connection information, and device ID and call information.[119] Google also stores the time stamps of when the apps are used and provides this info to the users via Google Takeout.

e)   Google+

110.   Google+ is a social media network launched in 2011 as a competitor to Facebook. Although Google does not release statistics on Google+'s active users, it is now primarily a place for niche communities.[120] A user can choose to follow other users, organize the users they follow into groups (e.g. best friends vs. work colleagues), start "Communities," or join existing ones (e.g. "Photography enthusiasts"). Posts from followed users and communities then appear in the user's home feed.

111.   Google Takeout shows several types of Google+ data that Google stores. Google compiles vCards from the profiles of all the people a user follows (in Takeout, this information is contained within the "Google+ Circles" folder). Google also collects in HTML format all content posted by a user, which is contained in the "Google+ Stream" folder of Takeout, as shown in Figure 21. Posted photos also are saved within Google Photos.

Figure 21: Example of Google+ posted content saved by Google

John Maple - Apr 26, 2018 - Google+ - Limited - Permalink
What are the best DSLR cameras?

f)   Translate

112.   Google Translate is a free machine translation service supporting over 100 languages that is available on the web and through apps for Android and iOS. It is also integrated into Google Assistant and Google Chrome, as well as being available to 3rd-party developers through a paid API.[121] Altogether, it serves more than 500 million monthly users.[122] If users have the Google Translate app on their phone, they can use the app to

---

[118] Swapna Krishna, "Google Duo allows you to call people who don't have the app," *Engadget,* Jan. 12, 2018, available at https://www.engadget.com/2018/01/12/google-duo-call-android-users-without-app
[119] Google informs the user of this access when the user downloads the app.
[120] Karissa Bell, "Google+ isn't dead and these are the people astill using it the most," *Mashable,* Jan. 18, 2017, available at https://mashable.com/2017/01/18/who-is-using-google-plus-anyway/#_IP0PXr.eiqZ
[121] "Google Cloud, pricing," *Google,* last accessed on August 15 2018, available at https://cloud.google.com/translate/pricing
[122] Gideon Lewis-Kraus, "The great A.I. awakening," *The New York Times,* Dec. 14, 2016, available at https://www.nytimes.com/2016/12/14/magazine/the-great-ai-awakening.html

translate languages within other apps, such as WhatsApp.[123] Although Google states that it does not track Google Translate web queries[124]—and these queries do not appear in a user's Search history or elsewhere in Google Takeout—Google's privacy policy does allow it to store them for short period of time and occasionally for longer period for debugging and other testing.[125]

g)   Calendar

113.   Google Calendar is a scheduling tool that enables users to keep track of their daily and weekly activities. It is widely used on both desktop and mobile devices, with more than 500 million downloads from the Google Play Store.[126] Personal information, such as an individual's name and contact information, is often associated with a Calendar user.

114.   By using calendars, users provide Google with details (such as the time, location, and contact information) for all participants of an event. Google states that the app has access to "read calendar events plus confidential information."[127] As part of this information collection, Google reads and stores the email addresses of all members included in a calendar event, regardless of their Google affiliation.[128] As long as one person on a calendar invitation is using Google Calendars, therefore, Google records the contact information for every other person on the invitation.

h)   Keep

115.   Google Keep is a note-taking tool that allows the user to take notes that sync between devices associated with their Google account. Keep has been downloaded more than 100 million times from the Google Play Store.[129] Google collects and stores all contents of the notes, as well as the time they were created.[130] Figure 22 shows Google Keep notes recorded by Google. Google scans and classifies the notes that are created based on their contents. Examples of classification categories are food, places, and travel.

---

[123] "Google Translate," *Google,* available at https://translate.google.com/intl/en/about
[124] "Google Translate help," *Google,* last accessed on August 15 2018, available at
https://support.google.com/translate/answer/6142479?co=GENIE.Platform%3DDesktop&hl=en&oco=0
[125] "Access to the Google Cloud API," *Google,* last accessed on August 15 2018, available at https://cloud.google.com/translate/faq
[126] "Google Calendar," *Google Play Store,* last accessed on August 15 2018, available at
https://play.google.com/store/apps/details?id=com.google.android.calendar
[127] "Google Calendar," *Google Play Store,* last accessed on August 15 2018, available at
https://play.google.com/store/apps/details?id=com.google.android.calendar
[128] "Download your data," *Google,* available at https://takeout.google.com/settings/takeout?pli=1
[129] "Google Keep," *Google Play Store,* last accessed on August 15 2018, available at
https://play.google.com/store/apps/details?id=com.google.android.keep&hl
[130] "Download your data," *Google,* available at https://takeout.google.com/settings/takeout?pli=1

Figure 22: Example of Google Keep notes, accessed from Google take out

```
        </style></head>
<body><div class="note"><div class="heading"><div class="meta-icons">

</div>
Apr 26, 2018, 11:06:04 AM</div>

<div class="content">Grocery list:<br>- pasta<br>- tomatoes<br>- lettuce <br>- salad
dressing <br>- salmon <br>- lemon<br>- capers <br>- Bread<br>- butter<br>- milk<br>-
eggs<br>- bacon<br>- OJ<br>- </div>

</div></body></html>
```

i)   Chromecast

116.   Like Apple TV, Google Chromecast is a device that acts as an interface to watch videos from a variety
of applications (e.g. Netflix, YouTube, Hulu, Play Store), as well as to project video from smartphones and
computers onto larger televisions and monitors. Every Cast device has a unique identifier that is associated with
a user's Google Account during registration.

117.   Google uses Chromecast to collect system activity, crash reports, and usage data, such as details about
the use of casting functionality of devices, including the apps and domains that are casted.[131] Chromecast uses
Google Cast, which is a software platform that enables seamless streaming of audio/video between devices on
the same network.[132] In addition to a multitude of other Google products (e.g. Google Home) that use Cast
functionality, the Cast platform is also used by 3rd-party devices using "Chromecast built-in" (e.g. TVs and
video gaming consoles[133]), that offer similar functionality. Google also collects usage data and crash reports
from 3rd-party Cast devices.[134]

j)   Google DNS

118.   Google launched a free Domain Name System (DNS)[135] service, called Google Public DNS, in
December of 2009. Google DNS is aimed at improving web browsing experience by enhancing speed, security,
and accuracy.[136] In December 2014, Google Public DNS was reported to be serving 400 billion responses.[137]

119.   To detect abuse (such as DDoS attacks) and to fix problems, Google Public DNS keeps a temporary
log of full IP addresses that it deletes within 24-48 hours. For longer-term efforts to debug and prevent abuse,

---

[131] "Chromecast help," *Google,* last accessed on August 15 2018, available at
https://support.google.com/chromecast/answer/6076570?hl=en
[132] "Google Cast," *Google,* last accessed on August 15 2018, available at https://developers.google.com/cast
[133] "What is Google Cast and Chromecast," *Shield,* last accessed on August 15 2018, available at https://shield.nvidia.com/blog/what-is-googlecast-chromecast
[134] "Chromecast help," *Google,* last accessed on August 15 2018, available at
https://support.google.com/chromecast/answer/6076570?hl=en
[135] DNS services translate domain names into IP addresses and thus are necessary to navigate the web.
[136] "Google Public DNS," *Google,* last accessed on August 15 2018, available at https://developers.google.com/speed/public-dns/faq
[137] "Google Public DNS and location-sensitive DNS responses," *Google Webmaster Central Blog,* Dec. 15, 2014, available at
https://webmasters.googleblog.com/2014/12/google-public-dns-and-location.html

Google keeps non-personally-identifiable city/metro-level location information for two weeks, and randomly samples a small subset for permanent storage.[138]

k)   Google Wi-Fi router

120.   Google began rolling out a mesh Wi-Fi router, Google Wi-Fi, in December 2016. Mesh routers allow a user to extend access to a Wi-Fi network across a larger area with additional connected routers. By December of 2017, Google Wi-Fi became the best mesh Wi-Fi system in the USA according to data from the NPD Group.[139] The information it collects[140] falls into the following three categories:

- Cloud services, which include broadcast information from connected devices (such as a device name like "Jane's iPhone"), infer information from connected devices (such as manufacture's name like Samsung), connection status, data transfer speed and historical consumption, network settings and information about wireless environment (e.g. other routers in the area). It does collect connected device information and data usage.
- Wi-Fi stats, which include anonymous data usage, crash reports and device performance information.
- Wi-Fi app stats, which includes usage and crash reports.

121.   According to Google, the Wi-Fi router does not track the websites visited or collect the content of network traffic.[141]

l)   Nest

122.   In January 2014, Google acquired Nest, which is a home automation company.[142] Nest's product line includes many smart home devices, including thermostats, cameras, doorbells, alarm systems, locks and smoke/CO detectors.[143] In addition, Nest lists more than 100 3rd-party products that can integrate with Nest, ranging from refrigerators to beds.[144]

123.   Nest devices collect a variety of information, including not only users' direct adjustments to the devices, but also data on the environment within the home. For example, the Nest Learning Thermostat collects data (such as temperature, humidity, ambient light, and movement) and thus knows when people are at home and even in what rooms.[145] When a user connect 3rd-party products that integrate with Nest, Nest shares

---

[138] "Google Public DNS," *Google,* available at https://developers.google.com/speed/public-dns/privacy

[139] Jillian D'Onfro, "The surprising use case that has made Google Wifi one of the company's sleeper hits," *CNBC,* Dec. 18, 2017, available at https://www.cnbc.com/2017/12/18/google-wifi-mesh-technology-sales-stats.html

[140] "Google Wifi help," *Google,* last accessed on August 15 2018, available at https://support.google.com/wifi/answer/6246642?hl=en

[141] "Google Wifi help," *Google,* last accessed on August 15 2018, available at https://support.google.com/wifi/answer/6246642?hl=en

[142] "Google to acquire Nest," *Alphabet,* Jan. 13, 2014, available at https://abc.xyz/investor/news/releases/2014/0113.html

[143] Nest homepage, available at https://nest.com/

[144] "Works with Nest," Nest, last accessed on August 15 2018, available at https://nest.com/works-with-nest/

[145] "Privacy statement for Nest products and services," *Nest,* last accessed on August 15 2018, available at https://nest.com/legal/privacy-statement-for-nest-products-and-services/

information with those parties but informs the user about what information is being shared.[146] Nest does not share data with other 3rd-parties, such as partner energy or insurance companies, without first gaining a user's consent.[147]

124.   On its website, Nest states that Nest accounts and Google accounts are not linked (unless a user chooses to integrate with Google products and services) and that Google does not sell Nest data. Recently, however, data sharing concerns have arisen from an announcement[148] by Google concerning the merger of Nest and Google hardware teams.[149] In addition, concerns have been raised in the media about the future links between Google, Nest, and 3rd-party electrical and insurance companies.[150]

m)   Google Fiber

125.   Google Fiber is a broadband, Internet protocol (IP) TV, and Voice-Over-Internet-Protocol (VOIP) phone service connecting users via ultra-high-speed fiber-optic networks that extend all the way to their residences,[151] known as Fiber Internet, Fiber TV, and Fiber Phone, respectively. Google's efforts to deploy extensive networks of fiber optic cables were hampered by physical costs and negotiations with local municipalities. Google Fiber is therefore now expanding to new cities via Webpass (an Internet service provider acquired by Google), which delivers similarly high speeds through existing wireless and Ethernet technologies.[152]

126.   Fiber Internet collects technical information connected to a user's Google Account, but does not share account details with other Google properties without the user's additional consent.[153] Fiber Internet requires user consent before associating a user's Google Account with other information, such as sites visited or content of communications.[154]

---

[146] "Privacy statement for Nest products and services," *Nest,* last accessed on August 15 2018, available at https://nest.com/legal/privacy-statement-for-nest-products-and-services/
[147] "Privacy statement for Nest products and services," *Nest,* last accessed on August 15 2018, available at https://nest.com/legal/privacy-statement-for-nest-products-and-services/
[148] Rick Osterloh, "Nest to join forces with Google's hardware team," *Nest,* Feb. 7, 2018, available at https://blog.google/topics/hardware/nest-join-forces-googles-hardware-team/
[149] Leo Kelion, "Google-Nest merger raises privacy issues," *BBC,* Feb. 8, 2018, available at http://www.bbc.com/news/technology-42989073
[150] Casey Johnston, "What Google can really do with Nest, or really, Nest's data," *Ars Technica,* Jan. 15, 2014, available at https://arstechnica.com/information-technology/2014/01/what-google-can-really-do-with-nest-or-really-nests-data/
[151] Ryan Waniata, "Comcast killer: Google Fiber touches down in Austin with its new TV and internet devices," *Digital Trends,* Dec. 3, 2014, available at https://www.digitaltrends.com/home-theater/google-fiber-tv-hands-on
[152] Nick Statt, "Google Fiber-owned Webpass is bringing its wireless gigabit internet to Denver," *The Verge,* Feb. 22, 2017, available at https://www.theverge.com/2017/2/22/14703142/google-fiber-webpass-denver-expansion-gigabit-Internet and https://gizmodo.com/what-happened-to-google-fiber-1792440779
[153] "Google Fiber privacy notice," *Google,* last accessed on August 15 2018, available at https://fiber.google.com/legal/privacy
[154] "Google Fiber privacy notice," *Google,* last accessed on August 15 2018, available at https://fiber.google.com/legal/privacy

127.   Fiber TV collects information on programs and applications used and associates it with the user's Google Account.[155] Likewise, Fiber Phone collects usage information (e.g. logs of call history, voicemails, SMS messages, and recorded conversations) and associates it with a user's Google Account.[156] Although this information is not shared with 3rd-parties unless a user provides consent, information may be shared with 3rd-parties for external processing and for legal reasons. While Google does not explicitly mention the use of Fiber TV/phone for ad targeting, its general privacy policy does allow the use of collected personal information for targeting purposes. Moreover, Google states it will share Google Fiber user's non-personal identifiable information publicly with content providers, publishers, advertisers, and/or connected sites.[157]

D.   Method for location traffic monitoring

128.   To capture the requests being sent to Google server domains from a mobile phone, our study employs a "man-in-the-middle" (MITM) technique using the "MITM Proxy" tool. While previous studies that analyze similar data employed a Wi-Fi hotspot to act as an intermediary between mobile phone and Google servers, the present study uses a virtual private network (VPN) on a mobile phone to analyze data sent through Wi-Fi networks as well as the cellular network.

Figure 23: Example VPN setup used to analyze data shared with Google
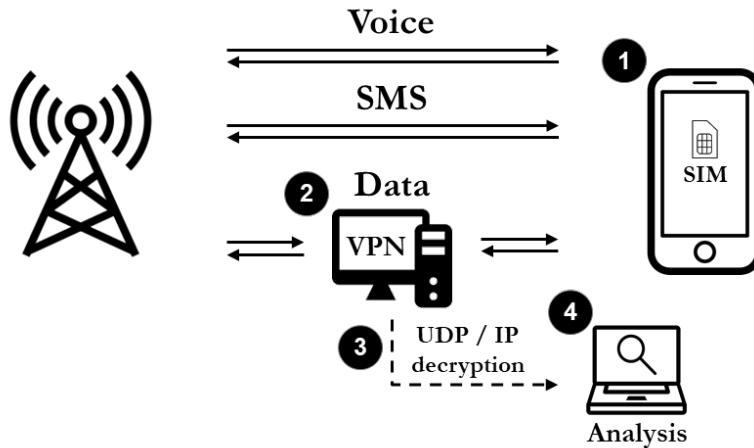
The specific steps performed to configure and conduct the experiments are described below:

1.   The mobile devices used in the data collection experiments[158] were factory reset to ensure that no previously installed applications or adjusted settings affected traffic to and from the phone. Upon

---

[155] "Google Fiber privacy notice," *Google,* last accessed on August 15 2018, available at https://fiber.google.com/legal/privacy
[156] "Google Fiber privacy notice," *Google,* last accessed on August 15 2018, available at https://fiber.google.com/legal/privacy
[157] "Google Fiber privacy notice," *Google,* last accessed on August 15 2018, available at https://fiber.google.com/legal/privacy
[158] Devices include an LG X Power with Android 6.0 version installed and an iPhone 5 with iOS 10.3.3 installed

reactivation, the devices were configured with the suggested default settings. The devices were then equipped with new SIM cards to obtain new cell phone numbers.

2. A VPN connection was setup with a remote proxy computer using VPN settings/functionality provided by the phone operating system. An IPsec/LT2P with a PSK authentication setup was chosen. The VPN configuration enabled the remote proxy to intercept and record the data transmitted from the mobile phones. Due to the nature of the type of signals emitted from a phone, the VPN set up is unable to intercept voice and SMS data sent from the mobile devices. However, it captured all TCP traffic to and from the device, including HTTP and HTTPS traffic.

3. HTTPS software certificates were installed on the mobile devices to enable decryption of the data traffic captured. VPN configuration allowed the routing of all HTTP and HTTPS traffic through the mitmproxy program[159] using iptables.[160] This program then performed SSL decryption using its own certificate to decrypt the traffic and dump it to HAR (HTTP Archive) files for analysis.

4. Analysis of decrypted HTTP and HTTPS traffic data mainly involved categorization of server requests into key segments using the request header info. Tables 5 and 6 detail the traffic headers that were identified as transmitting data to/from Google and Apple.

129.   In specific cases, requests to Google were further decoded to analyze the information that was passed at a more granular level. One specific request to Google that was further decoded was the "Google location API," designated by the /loc/m/api endpoint. The location specifications were reverse engineered by removing the message header and decoding the compressed protobuf message.[161] The decoded location API contained Wi-Fi and network scans that were used to determine the location of the device.

Table 5: Notable Google server domains communicating with mobile phone devices

Segment	Pathway header	Description
Ad domains	doubleclick.net	Sends data to and from DoubleClick
	google-analytics.com	Sends data to and from GA
	googletagmanager.com	Implements webpage tags
	googletagservices.com	Implements webpage tags
	googlesyndication.com	Retrieves and displays ads
	adservice.google.com	Calls the AdWords network

---

[159] https://mitmproxy.org/

[160] "iptables(8) – Linux man page," *Die.net,* available at https://linux.die.net/man/8/iptables

[161] Additional information on the decoding method can be found here: "Reverse engineering: Google Location protobuf specifications," *Esther Codes,* accessed March 2018, available at
https://web.archive.org/web/20180213201547/https://esther.codes/reverse-engineering-google-location-gms-specification/

	google.com/ads/	Ad measurement and user lists
	gstatic.com	Loads ads on the page
	google.com/adsense	Calls AdSense
	google.com/pagead	Serves page ads
Location	google.com/loc/m/api	Sends back nearby network and Wi-Fi information
	googleapis.com/userlocation/v1/reports	Sends back user movement information (i.e. walking, running, biking, driving, etc.)
	googleapis.com/placesandroid	Matches determined location with businesses, etc. (Google Places)
	maps.googleapis.com/maps	Retrieves detailed information based on a place ID or a place search
	clients4.google.com/glm/mmap	Sends user's location information to retrieve map data
Google Play API	play.googleapis.com/log/batch	Device activity logging information
	play.googleapis.com/play/log/timestamp	Updates a cookie and reports the time
	play.googleapis.com/play/log?format	Play Store/Services log upload
Device auth. and upload	googleapis.com/batch	Device information and updates
	clients4.google.com/chrome-sync	Chrome browser synchronization
	googleapis.com/experimentsandconfigs	testing/experiment config download
	android.clients.google.com/backup/backup	Device backup
	android.clients.google.com/auth	Device authorization
	android.clients.google.com/checkin	Device identifying information and activity
	android.clients.google.com/	Authentication with Google services
Other	cdn.ampproject.org	Retrieving data from the AMP CDN
	google.com/xjs	Communication with Google Search
	google.com/gen	Communications with Google Search that transmit cookie data
	clients4.google.com/ukm	Chrome speed information
	inbox.google.com/sync	Mail synchronization
	mail.google.com/mail/ads	Mail ad refresh
	google.com/complete/search	Sends character level information to enable the search autocomplete function
	Googleapi.com/	Other Google APIs include Google services (i.e. YouTube, Calendar, etc.)

	Google.com/	Other miscellaneous calls to Google's domain

Table 6: Notable Apple server domains communicating with mobile phone devices

Segment	Pathway header	Description
Location	geosrc=wifi,73.xxx&kb_ime=en_US&key=beagle1626&latlng=40.xxx,-74.xxx&locale=en_US	Passes location coordinates back to Apple when using the browser
	cl2.apple.com	Calls to the core location server
	gs-loc.apple.com	Apple location services
App store	us-east-1.blobstore.apple.com/apple	Communicates with the Apple store; includes Apple ID
Device auth. and upload	mesu.apple.com/assets/com_apple_MobileAsset	Details mobile configurations and settings
	bookmarks.icloud.com	Syncs mobile behavior with the cloud
	ckdatabase.icloud.com/api	Communicates device authorization tokens and syncs with iCloud
	keyvalueservice.icloud.com/sync	Syncs mobile device behavior
Other	api-glb-nyc.smoot.apple.com/	Miscellaneous Apple APIs
	gsp64-ssl.ls.apple.com	Provides device information when the phone accesses websites via Safari
	gspe35-ssl.ls.apple.com/geo_manifest/dynamic/config?application=geod	Loads map tiles, but does not pass location information
	configuration.apple.com/configurations/pep/config/geo/networkDefaults	Communicates the settings of the location collection tools

    E.   **Google sign in authentication sequence**

Figure 24: Authentication sequence
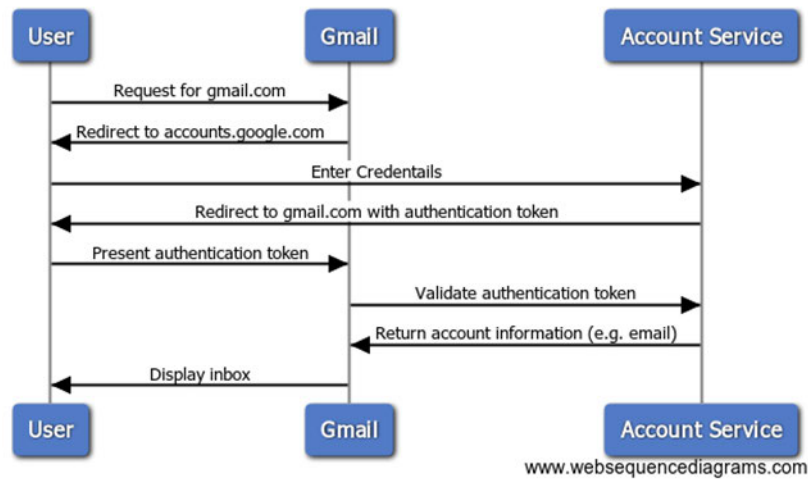
F.   **Usage profile for mobile data collection experiments**

130.   A usage profile was designed to simulate a typical user's interaction with their mobile phone throughout the course of a day. A variety of statistics that describe peoples' online behavior and mobile phone usage were integrated to create the profile, as described below.

131.   The designed profile visited 45 webpages during the course of the day based on website visit statistics from a 2010 Nielsen study, which indicates that the average person visits 88 webpages per day[162] and a 2017 Stone Temple study, which states that roughly 50-55% of webpage visits come from mobile devices.[163] The 45 webpage visits were evenly split between 5 top non-Google news and sports domains.[164] When the phone was not being used to visit webpages the browser was left running in the background of the phone. The resulting usage profile represents a conservative user as the number of webpage visits per day is likely to have increased since the 2010 Nielsen study.

132.   The usage profile also included a variety of non-Google mobile applications. Top non-Google applications were selected from the social media, shopping, travel, and health categories. These applications included Facebook, Instagram, Snapchat, Pinterest, Amazon Shopping, Walmart, Starbucks, Yelp, and Six Pack

---

[162] "Nielsen provides topline U.S. web data for March 2010," Nielsen, April 2010, available at
http://www.nielsen.com/us/en/insights/news/2010/nielsen-provides-topline-u-s-web-data-for-march-2010.html
[163] Eric Enge, "Mobile vs desktop usage: mobile grows but desktop still a big player in 2017," *Stone Temple,* April 2017, available at https://www.stonetemple.com/mobile-vs-desktop-usage-mobile-grows-but-desktop-still-a-big-player-in-2017/
[164] The domains selected were New York Time, CNN, The Guardian, ESPN, and Crickbuzz. The websites were identified by using Alexa's lists, available at https://www.alexa.com/topsites/category

50

in 30 Days. These apps were opened periodically throughout the day to simulate a typical user who spends approximately 2.5 hours in mobile app per day, as reported by eMarketer.[165]

G.   Past articles that relate to Google's data collection practices

Table 7: Summary of other Google data collection studies

Title	Relevant findings	Author, Date
AP Exclusive: Google tracks your movements, like it or not[166]	Google is tracking users' location even when location services are disabled	Ryan Nakashima August 2018
Australian regulator investigates Google data harvesting from Android phones[167]	Google "harvest" about 1GB of data from Android devices per month	Oracle May 2018
How to Keep Google From Owning Your Online Life[168]	It is very difficult for the average consumer to avoid Google products	WSJ, May 2018
Google tracking phones even when they are disconnected?[169]	Google tracks phones even when phones are "disconnected" (no SIM cards, airplane mode, Wi-Fi off)	Fox News, Feb. 2018
Google collects Android users' locations even when location services are disabled[170]	Google collects Android location when location services are turned off	Quartz Nov. 2017

---

[165] "eMarketer reveals new estimates for mobile app usage," *eMarketer,* April 2017, available at https://www.emarketer.com/Article/eMarketer-Unveils-New-Estimates-Mobile-App-Usage/1015611

[166] Ryan Nakashima, "AP Exclusive: Google tracks your movements, like it or not," *AP*, August 13, 2018, available at https://apnews.com/828aefab64d4411bac257a07c1af0ecb

[167] Anne Davis, "Australian regulator investigates Google data harvesting from Android phones," *The Guardian,* May 13, 2018, available at https://www.theguardian.com/technology/2018/may/14/australian-regulator-investigates-google-data-harvesting-from-android-phones

[168] David Pierce, "How to Keep Google From Owning Your Online Life," *The Wall Street Journal,* May 8, 2018, available at https://www.wsj.com/articles/how-to-keep-google-from-owning-your-online-life-1525795372

[169] Brett Larson, "Google tracking phones even when they are disconnected?," *Fox News,* Feb 11, 2018, available at http://video.foxnews.com/v/5731183327001/?#sp=show-clips

[170] Keith Collins, "Google collects Android users' locations even when location services are disabled," *Quartz,* November 17, 2017, available at https://qz.com/1131515/google-collects-android-users-locations-even-when-location-services-are-disabled/

Google is permanently nerfing all Home Minis because mine spied on everything I said 24/7[171]	The Google Home mini was saving recording when the device was not activated with "OK Google" *Google claims to have resolved the issue	Artem Russakovskii Oct. 2017
Online Tracking: A 1-million-site Measurement and Analysis[172]	Google can track users ~80% of websites using its cookies.	Princeton University 2016
Why Do Android Smartphones Guzzle the Most Data?[173]	Android devices consume more data (2.2GB/month) than other smartphones	Ericsson Dec. 2013
Data leakage from Android smartphones[174]	Android passes anonymous IDs along with devices IDs such as Mac address and IMIE	Lasse Øverlier June 2012

H.   Clarifications

133.   Our understanding of the data being sent to Google through its Android platform is limited to Android 6.0 version only. This study does not capture any updates/patches that may have been implemented on later versions that may affect Android's communications with the Google servers. While new versions of Android are currently present in the market, Android 6.0 is still the most widely used version.[175] Additionally, while we took utmost precaution for classifying the pathway headers by their purpose (e.g., location, ad, device upload, app store), it is possible that some headers may serve multiple purposes (e.g., ad as well as location). These aspects are not captured in our study. Consequently, the description presented for these headers may not be exhaustive with respect to the purpose they serve.

I.   About the author

134.   Professor Douglas Schmidt is a software system expert with over 30+ years conducting, supervising, and researching the development of software for distributed middleware systems and their applications in

---

[171] Artem Russakovskii, "Google is permanently nerfing all Home Minis because mine spied on everything I said 24/7," *Android Police,* October 10, 2017, available at https://www.androidpolice.com/2017/10/10/google-nerfing-home-minis-mine-spied-everything-said-247/

[172] Englehardt, Steven, and Arvind Narayana, "Online Tracking: A 1-million-site Measurement and Analysis," *ACM CCS,* 2016, available at http://randomwalker.info/publications/OpenWPM_1_million_site_tracking_measurement.pdf

[173] Brian Chen, "Why Do Android Smartphones Guzzle the Most Data?," *The New York Times,* December 31, 2013, available at https://bits.blogs.nytimes.com/2013/12/31/why-do-android-smartphones-guzzle-the-most-data/

[174] Lasse Øverlier , "Data leakage from Android smartphones," *Norwegian Defense Research Establishment,* June 6, 2012, available at https://www.ffi.no/no/Rapporter/12-00275.pdf

[175] "Mobile & Tablet Android Version Market Share Worldwide," *statcounter*, available at http://gs.statcounter.com/android-version-market-share/mobile-tablet/worldwide

networking and security, machine learning and smart-grid, design patterns, and more. He has authored 10+ books and 600+ papers that have been collectively cited over 38,000 times. Professor Schmidt has over 30 years of experience teaching these concepts both in-classroom and online to over 200,000 students in total.

135.   Professor Schmidt has participated in 20+ prior expert engagements spanning expert report production and oral testimony both through deposition and at trial. His consulting work has ranged from patent and copyright litigation matters to advising both private and public entities on various issues relating to software infrastructure and design. He earned his PhD and MS in Computer Science from the University of California, Irvine in 1994 and 1990, respectively.

136.   Professor Schmidt is currently the Cornelius Vanderbilt Professor of Computer Science at Vanderbilt University. Prior to Vanderbilt, he held several directorial and C-level positions in both academic and industry settings including the Software Engineering Institute at Carnegie Mellon University, the Information Technology Office at the Defense Advanced Research Project Agency (DARPA), the Federal Government, as well as several technology start-ups.

Abortion

US states could ban people from traveling for abortions, experts warn

If supreme court weakens Roe v Wade, some states will take aim at people seeking procedures and medications out of state

Melody Schreiber

Tue 3 May 2022 06.00 EDT

As abortion bans proliferate in states around the US, some state legislatures are likely to go even further than just ending abortion in their jurisdictions – taking aim at the growing numbers of people seeking procedures and medications out of state, experts warn.

If, as the bombshell leak of its private vote suggests, the supreme court weakens or overturns Roe v Wade – the 1973 decision that established a constitutional right to abortion – in an upcoming decision on Mississippi's 15-week abortion ban, states will be left with a confusing patchwork of laws that will probably lead to legal challenges.

A fresh wave of restrictions will probably center around patients who leave their state to obtain legal abortions in other states, or who order medications to manage their abortions at home.

Lawmakers in Missouri weighed legislation early this year that would allow individuals to sue anyone helping a patient cross state lines for an abortion. The law was ultimately blocked in the state's legislature, but experts expect such legislation to gain more support if Roe is weakened or overturned.

"I think states are not going to rest with just saying 'there won't be abortions in our state.' I think they're going to want to ban abortion for their citizens as much as they can, which would mean stopping them from traveling," said David Cohen, professor at Drexel University's Kline School of Law and lead author of a forthcoming article on cross-state legal issues that could arise in the abortion context.

"We're going to see state-against-state battles that are really going to divide this country even deeper on this issue," he said.

If the supreme court overturns abortion protections, such travel bans might also be permitted to stand, Cohen said.

"The supreme court does not have well-developed case law regarding extraterritorial application of state law," he added in an email. A court that has gone so far as to overturn Roe, he said, "would likely take that unclear precedent in the direction that is most anti-abortion."

But banning travel would go against "basic American principles", he said. "You have freedom of travel in this country, and as long as you're following the law in the state where you are, you are legally OK" under current law. For instance, adults can gamble in states where it's legal, even if they're from states where it's not allowed.

gamble in states where it's legal, even if they're from states where it's not allowed.

If the constitutional right to abortion is reversed, more than half of states are likely to prohibit abortions, according to separate analyses by the Center for Reproductive Rights and the Guttmacher Institute.

Several states have recently passed abortion bans that would be unconstitutional under Roe, but could stand if the landmark ruling is overturned by the supreme court. Some have passed laws similar to Texas's ban on abortions at six weeks of pregnancy – around four weeks after conception, when most people don't know they are pregnant – while others are advancing legislation similar to the 15-week ban at the center of the supreme court case.

On Thursday, Oklahoma lawmakers passed a Texas-style ban that will take effect immediately after Governor Kevin Stitt signs it, expected to occur within days. Stitt signed another bill earlier this year that would make abortion illegal in nearly all circumstances, but that law would not take effect until August.

As state-based restrictions proliferate, traveling out of state for reproductive healthcare has become common. After the Texas law took effect last year, Planned Parenthood clinics in neighboring states saw an almost 800% increase in patients.

If Roe is weakened or overturned, "a lot of the states that are likely to lose access are surrounded by other states that are likely to lose access", said Mikaela Smith, a research scientist at the Ohio State University's College of Public Health and the lead author of new research on out-of-state abortion travel. That means patients may need to travel across several states to receive care.

That would also exacerbate existing inequities in healthcare, she said. "Folks who have the resources and have the financial means will be able to do the extra work to cross state lines and folks who don't, or don't have the connections or know how to access the care they need, just won't be able to."

States are also likely to crack down on other efforts to access care. In Texas, a law passed last year made it illegal to ship medication for self-managed abortion, including across state lines – another potential template for copycat legislation.

Since the US Food and Drug Administration (FDA) announced last year that it would continue its pandemic-era policy to allow medication abortion, also known as the "abortion pill", to be prescribed via telemedicine, the drugs have become a greater target from anti-abortion advocates. Medication abortion now accounts for the

majority of abortions in the US.

"Pills are going to be a major part of how people continue to get abortions after the supreme court rules, so I think that we'll see states trying to ban pills in all sorts of different ways," Cohen said.

Blue states are preparing for the upcoming decision by shoring up reproductive rights for patients and protections for providers.

Soon after Idaho passed a contested Texas-style ban, neighboring Washington enacted the first law to prevent lawsuits on performing or aiding an out-of-state abortion.

Bills are progressing through the Connecticut and Illinois legislatures to protect patients traveling from out of state and the providers who care for them, and a dozen bills are moving through the California legislature to make reproductive rights stronger and more accessible.

Best VPNs of 2022

Popular VPN Services

NordVPN »

Monthly Plan Cost
   $11.95/Month

Annual Plan Cost
   $4.92/Month

# of IP Addresses
   5,502+

Server Count
   5,200+

Simultaneous Connections
   6

See Review

Surfshark »

Special Offer: Get TWO additional months FREE on Two-Year Plans

Monthly Plan Cost
   $12.95/Month

Annual Plan Cost

Not Offered

# of IP Addresses
    3,000+

Server Count
    3,200+

Simultaneous Connections
    Unlimited

See Review

ExpressVPN »

Monthly Plan Cost
    $12.95/Month

Annual Plan Cost
    $8.32/Month

# of IP Addresses
    Varies

Server Count
    3,000+

Simultaneous Connections
    5

See Review

Virtual private networks (VPNs) have been around since the 1990s. Businesses used VPNs to provide remote workers with a secure connection while online. There were very few personal VPN subscriptions. Today, however, Cloudnet reports that almost one-third of all internet users use a VPN. Due to the coronavirus pandemic, VPN usage grew even more, and the market for VPNs is now expected to exceed $92 billion in 2027.

VPNs exist to help encrypt your data when you're using the internet. According to Cloudnet, 49% of users choose VPNs for general security, whereas 31% of users connect to public Wi-Fi through VPNs. Some respondents admitted using VPNs to bypass school or work internet restrictions. That's because VPNs provide coverage from the prying eyes of internet service providers (ISPs) and others who could be

tracking your activities on the web.

Not all VPNs, however, are the same. With few standards and laws to regulate them, it can be hard to tell which companies are worth your time and money.

Our guide shows you the Best VPN Services of 2022 and helps you pick the right service for you. Read on to learn about the security features of top-rated VPNs, such as ExpressVPN, NordVPN, and Surfshark.
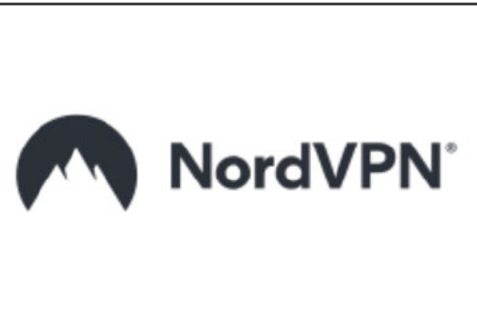
Prykhodov

Our Best VPNs of 2022 Rating

Compare the Best VPNs of 2022

We evaluated dozens of companies in search of VPNs that are trustworthy, easy to use, and have lots of security features. We included feedback from professional reviewers and consumers to create our rating of the Best VPN Services of 2022. See our summaries of each VPN service below, and visit each company's full review for more information.

ExpressVPN
Simultaneous Connections
5

NordVPN
Simultaneous Connections
6

Private Internet ACCESS®	
Simultaneous Connections 10	

IPVANISH	
Annual Plan $7.50/Month ($3.75/mo. For the first year) Simultaneous Connections Unlimited	

ExpressVPN	ExpressVPN Best VPN of 2022 (tie) 4.3 **U.S. News** Rating Monthly Plan $12.95/Month Annual Plan $8.32/Month Simultaneous Connections	View Plans

	5 Server Count 3,000+ 24/7 Support Yes	
	NordVPN Best VPN of 2022 (tie) 4.3 **U.S. News** Rating Monthly Plan $11.95/Month Annual Plan $4.92/Month Simultaneous Connections 6 Server Count 5,200+ 24/7 Support Yes	**View Plans**
	Surfshark Best VPN with Unlimited Connections 3.9 **U.S. News** Rating Monthly Plan $12.95/Month	**Special Offer: Get TWO additional months FREE on Two-Year Plans** **View Plans**

Annual Plan

Not Offered

Simultaneous
Connections

Unlimited

Server Count

3,200+

24/7 Support

Yes

Private Internet Access   View Plans

Best Low-Cost Annual
VPN Plan

3.9
    **U.S.
News** Rating

Monthly Plan

$9.95/Month

Annual Plan

$3.33/Month

Simultaneous
Connections

10

Server Count

25,000+

24/7 Support

Yes

IPVanish   View Plans

3.8
U.S.
News Rating

Monthly Plan

$10.99/Month

Annual Plan

$7.50/Month
($3.75/mo. For the
first year)

Simultaneous
Connections

Unlimited

Server Count

2,000+

24/7 Support

Yes

Best VPNs in Detail

ExpressVPN »

Best VPN of 2022 (tie)

Monthly Plan Cost
$12.95/Month

Annual Plan Cost
$8.32/Month

# of IP Addresses
        Varies

Server Count
        3,000+

Simultaneous Connections
        5

Pros

- Access to about 3,000 servers in 94 countries

- British Virgin Islands location

Cons

- Above-average price among the VPNs in our rating

- Only allows five devices to connect simultaneously

ExpressVPN: Tying for No. 1 in our Best VPNs of 2022 rating, ExpressVPN scores a 4.3 out of 5. Although it's relatively expensive at $12.95 a month or $8.32 per month annually, you get a lot for your money, including access to more than 3,000 servers in 94 countries. Because it's based in the British Virgin Islands, ExpressVPn is outside of the Five Eyes international intelligence-sharing agreement between the United States, United Kingdom, Canada, Australia, and New Zealand. The VPN provider is compatible with major operating systems, streaming services, and social media platforms. It also offers useful features like split tunneling. On the downside, it only allows five simultaneous connections. There's a 30-day money-back guarantee if you decide ExpressVPN isn't for you.

[NordVPN »](#)

Best VPN of 2022 (tie)

Monthly Plan Cost
      $11.95/Month

Annual Plan Cost
      $4.92/Month

# of IP Addresses
      5,502+

Server Count
      5,200+

Simultaneous Connections
      6

Pros

-   Extra privacy provided by Double VPN

-   Dedicated IP address available

Cons

-   Relatively high cost

-   Only six simultaneous connections

NordVPN: Also taking the No. 1 spot in our rating with a score of 4.3 out of 5 and located outside Five Eyes jurisdiction, Panama-based NordVPN costs $11.99 a month ($4.99 a month annually) and allows for six simultaneous VPN connections. One standout feature is NordVPN's Double VPN, which lets users send their traffic to two VPN servers. This process encrypts the information twice, which offers more privacy. NordVPN has about 5,000 servers worldwide, considerably more than ExpressVPN. For an additional $70 a year, you can add a dedicated IP address that will keep you from getting banned from your favorite websites for the actions of other people sharing the VPN company's IP addresses. Reviewers say NordVPN's interface is easy to use.

Surfshark »

![Surfshark logo]

Best VPN with Unlimited Connections

Special Offer: Get TWO additional months FREE on Two-Year Plans

Monthly Plan Cost
$12.95/Month

Annual Plan Cost
Not Offered

# of IP Addresses
3,000+

Server Count
3,200+

Simultaneous Connections
Unlimited

Pros

- Unlimited devices

- No extra charge for a static IP address

Cons

- High monthly cost

- Limited number of server locations

Surfshark: Surfshark ties for No. 3 on our Best VPNs list with a score of 3.9 out of 5. It rates the highest among the VPNs in our rating that offer an unlimited number of simultaneous connections. The VPN service provides several key features, including its Whitelister service to facilitate split tunneling. The monthly cost is

relatively high at $12.95, but a one-year subscription brings that down substantially to $2.49 a month. You can get a static IP address for no additional cost, and the "no borders" feature allows you to spoof your location to avoid monitoring or censoring by the government. Surfshark is compatible with a wide range of operating systems and browsers, including Chrome, Firefox, iOS, Android, and even FireTV. On the downside, with about 3,200 servers in 65 countries, it has fewer server locations than some other VPNs in our rating.

Private Internet Access »

Best Low-Cost Annual VPN Plan

Monthly Plan Cost
$9.95/Month

Annual Plan Cost
$3.33/Month

# of IP Addresses
Varies

Server Count
25,000+

Simultaneous Connections
10

Pros

- Includes free email breach monitoring

- Provides a one-year cloud storage subscription

Cons

- Based in the U.S. and thus subject to Five Eyes jurisdiction

-

Doesn't offer unlimited device connections

Private Internet Access: Private Internet Access also ties for No. 3 with a score of 3.9 out of 5. This budget-friendly VPN provider has the cheapest annual plan out of the companies in our Best VPNs of 2022 rating. For just $3.33 a month with an annual plan (or $9.95 per month on a monthly plan), Private Internet Access' subscription gives you 10 simultaneous connections with an array of VPN features. You also get free email breach monitoring, a one-year cloud storage subscription for your encrypted files, good speeds, and key privacy and security features like a kill switch, DNS leak protection, and a malware blocking add-on. A dedicated IP address is available for an additional $5 a month. Note that Private Internet Access is based in the U.S. and thus is under the jurisdiction of the Five Eyes alliance. However, like most VPNs, the company has a no-logging policy.

IPVanish »

IPVANISH

Monthly Plan Cost
    $10.99/Month

Annual Plan Cost
    $7.50/Month ($3.75/mo. For the first year)

# of IP Addresses
    40,000+

Server Count
    2,000+

Simultaneous Connections
    Unlimited

Pros

-
    Many IP addresses for better online privacy

-
    Unlimited simultaneous connections

Cons

- U.S.-based and thus under Five Eyes jurisdiction

- Not compatible with certain streaming services

IPVanish: Coming in at No. 5 in our rating with a score of 3.8 out of 5, U.S.-based IPVanish offers users access to more than 40,000 IP addresses. This helps protect anonymity online because it's unlikely that a given user will use the same IP address more than once. The VPN costs a reasonable $10.99 a month or $14.99 quarterly and allows an unlimited number of simultaneous device connections. IPVanish is compatible with social media, including Facebook, Instagram, Twitter, and YouTube. However, those who want to use [streaming services](#) are out of luck, as IPVanish won't work with popular ones like [Amazon Prime](#), [Disney+](#), and [Hulu](#). Also, on the downside, this VPN service has fewer servers than many of its competitors. But if these negatives don't bother you and your household has a lot of devices to protect, IPVanish is a good choice.

Windscribe »

Best Free VPN (tie)

Monthly Plan Cost
$9.00/Month

Annual Plan Cost
$4.08/Month

\# of IP Addresses
Not Available

Server Count
Not Available

Simultaneous Connections
Unlimited

Pros

-

Static IP address available for an extra cost

- Unlimited device connections, even with the free version

Cons

- Canada-based and thus under Five Eyes jurisdiction

- No live customer support

Windscribe: This VPN service ties for No. 6 in our rating with a score of 3.7 out of 5. Windscribe is based in Canada, which is under Five Eyes jurisdiction. Windscribe's annual plan costs a relatively reasonable $4.08 per month and is the cheapest VPN in our rating that lets you cover unlimited devices. A static IP address is available for an additional cost. Another Windscribe feature aims to avert browser tracking by adjusting or rotating the data used by the browser. No kill switch is offered, but the VPN service claims that its built-in firewall is more effective than a kill switch at preventing data leaks. Windscribe offers a free version that includes 10 gigabytes (GB) of data per month and also allows an unlimited number of connections. Another option allows you to "build a plan" at $1 per month for each location you are using. Note that Windscribe's money-back guarantee period is only three days.

ProtonVPN »

Best Free VPN (tie)

Monthly Plan Cost
$5.00/Month

Annual Plan Cost
$4.00/Month

# of IP Addresses
1,200

Server Count

1,546

Simultaneous Connections
    Up to 10

Pros

- Least expensive monthly plan among VPNs in our rating

- Offers a free version

Cons

- Only two device connections allowed on lowest tier

- No dedicated IP address available

ProtonVPN: With a score of 3.7 out of 5, ProtonVPN ties with Windscribe and CyberGhost in our rating. ProtonVPN's basic monthly plan is the least expensive among the VPN services in our rating at $4 a month. However, only two simultaneous connections are allowed, and features are limited. Higher-tier plans allow more simultaneous connections and additional features like peer-to-peer (P2P) torrenting and streaming service support. The most comprehensive Visionary plan is expensive at $24 a month, although it comes with an encrypted email service called ProtonMail. On the other end of the spectrum, ProtonVPN also offers a free version of its VPN. The free version is limited to one device and only 83 servers in 3 countries, but it has no advertisements or limits on data or speed.

CyberGhost »

Best VPN with Optional Security Suite

Monthly Plan Cost
    $12.99/Month

Annual Plan Cost
>$3.95/Month

# of IP Addresses
>6,600+

Server Count
>7,700+

Simultaneous Connections
>7

Pros

- Based in Romania outside of Five Eyes Jurisdiction

- Dedicated IP address available

Cons

- Relatively expensive monthly plan

- Only seven simultaneous connections

CyberGhost: Also tying for No. 6 with a score of 3.7 out of 5, CyberGhost is based in Romania and thus is not under the jurisdiction of the Five Eyes information-sharing alliance. This VPN service costs $12.99 a month, which puts it among the more expensive VPNs in our rating. However, if you're willing to sign up for a year, that price drops significantly to $4.29 a month, with even cheaper monthly rates for multiyear plans. Cyberghost allows seven simultaneous connections, offers 24/7 customer support, and provides the longest money-back guarantee in our ratings at 45 days. A dedicated IP address is available at an extra cost, and you can also add CyberGhost's Windows Security Suite. The security suite includes antivirus software, a privacy tool that lets you customize information-sharing settings, and a tool that tracks when apps on your laptop are due for an update.

PureVPN »

Monthly Plan Cost
      $10.95/Month

Annual Plan Cost
      $2.99/Month

# of IP Addresses
      300,000+

Server Count
      6,500+

Simultaneous Connections
      10

Pros

- Reasonably priced family plan

- Dedicated P2P servers

Cons

- Can't unblock Amazon Prime

- Customer support can be spotty

PureVPN: Coming in at No. 9 on our list with a score of 3.5 out of 5, PureVPN charges $10.95 per month for a monthly plan, $2.99 per month for 12 months, or $1.99 for 24 months on longer-term plans – the lowest multiplan cost in our ratings. Despite its low price, you get all the most commonly sought-after VPN functionality, including dedicated IP support, a kill switch, DNS leak protection, and split tunneling. PureVPN also offers optional DDoS protection and port forwarding. While you can connect an unlimited amount of devices, PureVPN limits simultaneous connections to 10. It has dedicated P2P servers in countries where

P2P is legal and offers dedicated streaming servers. The VPN service follows a strict no-log policy and is the only VPN service to gain KPMG's always-on no-log certification.

VyprVPN »

Best Business VPN Plan

Monthly Plan Cost
      $15.00/Month

Annual Plan Cost
      $8.33/Month

# of IP Addresses
      300,000+

Server Count
      700+

Simultaneous Connections
      5

Pros

- Switzerland-based VPN subject to strong privacy laws

- Offers a large number of IP addresses

Cons

- Relatively high cost for monthly subscription

- Only five devices can connect at once

VyprVPN: VyprVPN ties with TunnelBear and Hotspot Shield for No. 10 in our Best VPNs rating with a score of 3.4 out of 5. This VPN provider is based in Switzerland, which has strong privacy laws, plus VyperVPN has a no-logs policy that is confirmed by public audits. The company's monthly plans are relatively expensive at $15, while an annual plan comes to 8.33 a month (billed at $100 a year). VyprVPN only offers five simultaneous connections, which is on the low side. However, it provides more than 300,000 shared IP addresses, far more than any other VPN service in our rating. If five simultaneous connections meet your needs, VyprVPN may be a good affordable option for you. There's a 30-day money-back guarantee if you sign up and change your mind.

TunnelBear »

Monthly Plan Cost
　　$9.99/Month

Annual Plan Cost
　　$4.99/Month

# of IP Addresses
　　Not Available

Server Count
　　Not Available

Simultaneous Connections
　　Up to 5

Pros

- Free version offered

- Easy to use for beginners

Cons

- Based in Canada and thus subject to Five Eyes jurisdiction

- Can't use with streaming services or social media

TunnelBear: TunnelBear also ties for No. 10 in our rating with a score of 3.4 out of 5. This VPN provider is located in Canada, which is a Five Eyes country. The price is less than average among the companies in our rating, with a monthly plan costing $9.99 and an annual plan that works out to $4.99 a month. If you're willing to sign up for three years, the cost drops to $3.33 a month. There's a free version, although this is limited to 500 MB of monthly data, which isn't enough for many users. TunnelBear is compatible with all major operating systems, but not with social media or streaming services. The VPN provider has more than 3,000 servers in 49 countries, on par with some other companies in our rating but less than others. However, you can only have five simultaneous connections, and TunnelBear lacks a dedicated IP address option and other advanced features.

Hotspot Shield »

Monthly Plan Cost
   $12.99/Month

Annual Plan Cost
   $7.99/Month

# of IP Addresses
   Not Available

Server Count
   3,200+

Simultaneous Connections
   Up to 25

Pros

- Free single-device VPN offered

- Premium plan includes security suite features

Cons

- Relatively high monthly cost

- Only five simultaneous connections

Hotspot Shield: Hotspot Shield completes the three-way tie for No. 10 in our rating with a score of 3.4 out of 5. It costs $12.99 a month, or $7.99 a month on the annual plan (billed as $95.88 a year). You're only allowed five simultaneous connections on an individual plan, but you get extra security features like spam-call blocking and a password manager. A family plan allowing up to 25 simultaneous connections is available for $11.99 a month. If you only need basic VPN functionality, consider Hotspot Shield's free plan, which gives you military-grade encryption on one device with a daily data limit of 500 megabytes (MB). All plans are optimized for Netflix, YouTube, Hulu, and other streaming services, and speeds are relatively fast at up to 1 gigabit per second.

Our Best VPNs for iPhone Rating

Best VPNs for iPhones Table of 2022

ExpressVPN »
Simultaneous Connections 5
Server Countries 94
Server Count 3,000+
24/7 Support Yes
View Plans »

NordVPN »
Simultaneous Connections 6
Server Countries 59
Server Count 5,200+
24/7 Support Yes
View Plans »

Surfshark »
Simultaneous Connections Unlimited
Server Countries 65
Server Count 3,200+
24/7 Support Yes
View Plans »
Special Offer: Get TWO additional months FREE on Two-Year Plans

IPVanish »
Simultaneous Connections Unlimited
Server Countries 53
Server Count 2,000+
24/7 Support Yes
View Plans »

Our Best VPNs for iPhone rating consists of the highest-rated VPNs from our Best VPNs of 2022 rating that are compatible with iOS. If you have an iPhone or iPad, these VPNs should be on your shortlist.

Our Best Free VPNs of 2022 Rating

Best Free VPNs of 2022

Windscribe »
Simultaneous Connections Unlimited
Server Countries 63
Server Count Not Available
24/7 Support No
See Review »

ProtonVPN »

Case 4:20-cv-03664-YGR   Document 928-20   Filed 04/19/23   Page 303 of 405

Simultaneous Connections Up to 10	
Server Countries 63	
Server Count 1,546	
24/7 Support No	
View Plans »	

TunnelBear »
Simultaneous Connections Up to 5
Server Countries 49+
Server Count Not Available
24/7 Support Yes
View Plans »

If you don't need extra features like high data and P2P limits or fast connection speeds, a free VPN could meet your needs. Our rating of the Best Free VPNs of 2022 is taken from our rating of the Best VPNs of 2022. All of our Best Free VPNs still allow you to privately search and encrypt data sent over the web.

That said, don't use just any free VPN, because some of them might compromise your online security. It isn't worth taking that risk just to save a few dollars a month. So before signing up for a free VPN, review our rating of the Best Free VPNs. It will provide all the information you need to make an informed decision about choosing a free or cheap VPN that's reputable and will keep you safe online. We also discuss VPNs with trial periods and money-back guarantees.

What Is a VPN?

A VPN, or virtual private network, is software that conceals your online activities from your internet service provider (ISP) and hackers who might want to spy on you or steal your personal data. Without a VPN, an internet-connected device like a laptop or tablet sends unencrypted traffic through your ISP's servers, which means your ISP knows what you do online. Plus, the information you send is vulnerable to being intercepted. A VPN solves this problem by redirecting your internet traffic through its own network of servers first to disguise any information that could be used to identify you. This means that when you use a VPN, you can use the internet more anonymously.

Every device connected to the internet has a unique IP address associated with it. An IP address identifies a device much like a fingerprint identifies a person. In addition, an IP address normally isn't private. That means that someone can use your device's IP address to trace browsing history, geographical location, and other personal information back to you. Using a VPN solves this potential problem by

replacing your device's IP address with one that the VPN service provides. So rather than someone seeing your digital fingerprints, they will only see those of the VPN provider.

A VPN isn't a complete online security solution, however. While a virtual private network does provide more online privacy by helping to keep you anonymous while using the internet, there is no way to guarantee anonymity 100%. That simply isn't possible online. Still, one of the best ways to maintain online privacy when using the web is to subscribe to a VPN service.

Also realize that there are other online cybersecurity threats that a VPN won't protect you from at all. In particular, a VPN won't keep malware like viruses and ransomware from infecting your computer. For that, you need antivirus software.

How Does a VPN Work?
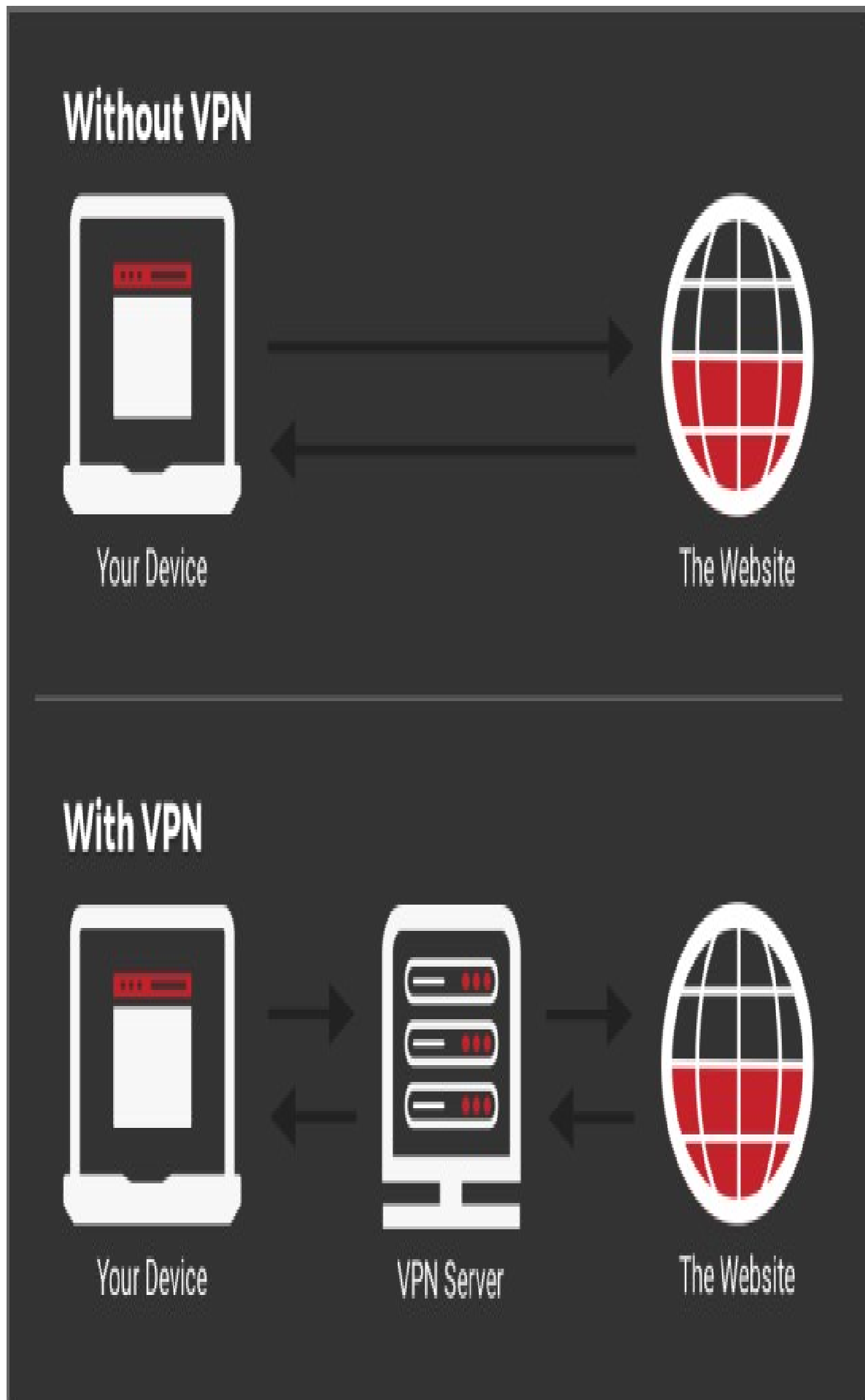
(USN&WR)

A VPN works by encrypting and hiding your online activity. Imagine that there's a tunnel between your internet-connected device and your ISP's server. Any search query or website you enter into your browser travels through the tunnel to your ISP. The ISP's server then retrieves the information you ask for and sends it back through the tunnel to your device. Because your device and the server are directly linked through the tunnel, your ISP or a hacker can see what you're doing on the internet and intercept your data.

A VPN makes this process more secure by encrypting your internet query and sending it to the VPN's server first. The VPN then sends your query to your ISP's server through the secure tunnel, disguised as traffic from one of the VPN's IP addresses. The ISP's server fetches the search result or website you want and sends it to the VPN's server, where it is unencrypted and sent to you. Because the VPN communicates your internet search for you, no one can associate that search with you or your devices.

How Does a VPN Keep Your Data Safe?

Best VPNs Location Data

ExpressVPN »
Server Locations 160
Server Countries 94
Country/Jurisdiction British Virgin Islands
Five Eyes HQ No

NordVPN »
Server Locations Not Available
Server Countries 59
Country/Jurisdiction Panama
Five Eyes HQ No

Surfshark »
Server Locations Not Available
Server Countries 65
Country/Jurisdiction British Virgin Islands

Five Eyes HQ No

IPVanish »
Server Locations 75+
Server Countries 53
Country/Jurisdiction USA
Five Eyes HQ Yes

A VPN's most important task is to keep your internet activity, identity, and location private. This prevents your ISP, advertisers, and hackers from viewing and tracking what you do online. It also prevents a restrictive government or organization from blocking what you're trying to do online.

"When using a VPN, you're making your Internet traffic pass through the VPN provider's servers before reaching your destination on the Internet," explains the Electronic Frontier Foundation, a nonprofit organization that advocates for user privacy and free speech online. "Your ISP will see that you're connecting to a VPN provider, but won't be able to see what you're ultimately connecting to. This is important to understand because you're exposing your entire Internet activity to the VPN provider and shifting your trust from the ISP to the VPN."

Think of a VPN as a private tunnel between you and the website you want to visit. To create this tunnel, a VPN uses several types of technology, one of which is 256-bit AES encryption. This type of encryption scrambles your data on one end of the tunnel and unscrambles it on the other. According to tech giant IBM, AES encryption is so secure that it's used by the U.S. government.

Do I Need a VPN?

VPNs are good for:

- Protecting your passwords and privacy when using a public Wi-Fi network

- Connecting to your employer's network when you're working remotely

- Preventing your internet service provider from seeing your search history and data use

-

Keeping your ISP from throttling, or slowing down, your internet speed

-

Concealing your location and identity when you're in a restrictive country

VPNs are not good for:

-

Keeping your devices from being infected by malware and viruses

-

Providing complete online anonymity

-

Accessing streaming services or other subscription-based content without an account

You need a VPN if you want to protect your laptop, tablet, or devices from hackers while they're connected to a public Wi-Fi network. You also need a VPN to access websites censored by the country you're located in, or when you want to appear to be connecting from another physical location.

For most people, a VPN is most important for privacy when using public Wi-Fi hotspots. The Federal Trade Commission (FTC) notes that public Wi-Fi networks aren't secure, making it easy for a hacker with the right equipment to intercept your data.

How to Choose a VPN

ExpressVPN »
Static IP
Kill Switch
DNS Leak Protection
Split Tunneling
P2P Functionality/Torrenting

NordVPN »

Static IP
Kill Switch
DNS Leak Protection
Split Tunneling
P2P Functionality/Torrenting

Surfshark »
Static IP
Kill Switch
DNS Leak Protection
Split Tunneling
P2P Functionality/Torrenting

IPVanish »
Static IP
Kill Switch
DNS Leak Protection
Split Tunneling
P2P Functionality/Torrenting

Because you entrust a VPN with personal information, take as much care in selecting a VPN service as you would a home security company. When choosing a VPN, consider:

- What features you need
- What devices you will use with it
- What you want to do with it
- How much it costs

To understand what makes a reliable VPN, it's helpful to first understand how this

technology works. "When you use a VPN app, data sent from your phone – be it your browsing data or the apps you are using – is routed through servers located elsewhere," according to the FTC. "A VPN app can make traffic from your phone to a website you visit appear to come from a server operated by the VPN provider, rather than directly from your phone. Some VPN apps also encrypt the data sent between your phone and the VPN server."

What features do you need?

Consider these other factors when evaluating a VPN company:

Privacy policy: The FTC says that if you're using a VPN app to keep your internet traffic private, review the app's terms and conditions and its privacy policy to see if it shares information with third parties like advertisers (and if so, which ones).

Data logs: Also look for a VPN company's policy on data logging, which is often included in its privacy policy. There are typically two types of data that may be collected. The first type is your connection log, which may include information such as the IP address you use to connect from, the websites you visit, the length of time you're connected, and the VPN servers you connect to. Usually (but not always) a VPN with a zero-logs policy doesn't record this information. VPNs do often keep track of minimal user data (such as your username and email address), and some log data such as the VPN app you use and crash reports, in the name of troubleshooting and user experience.

Andy Maxwell, author of the blog, TorrentFreak, says VPNs can be ordered by a court to hand over their customers' details but it is not always straightforward. According to Maxwell, good VPNs don't carry logs. However, in the event of any questionable streaming of events or similar activity that could warrant government inquiry, it's best to know where your VPN stands on data logs.

Country of jurisdiction: The country where the VPN has its headquarters dictates what information the VPN is legally required to log, and it can also impact how easily the government can get hold of that information. For example, the five countries that belong to the Five Eyes alliance (Australia, Canada, New Zealand, the U.S., and the U.K.) have an agreement to work together for surveillance and intelligence sharing.

VPN protocols: Thinking again of a VPN as a tunnel, a VPN protocol is like the blueprints for the tunnel. Most VPNs automatically select the best protocol for your needs, though advanced users may want the ability to pick a specific protocol. The best VPN protocols currently include OpenVPN and L2TP, which are more secure than older ones such as PPTP. Learn more about which VPN protocol is best from ExpressVPN, our top-rated VPN service.

Kill switch: If your VPN connection drops, your information is no longer secure. A kill switch prevents the accidental leakage of any data by blocking your internet connection if this happens. When your VPN is working again, its auto-connect feature instantly reinstates your internet connection.

Number of IP addresses: An IP address is a number that identifies your computer (or mobile device) and its current location. A VPN service substitutes your real IP address with one of its own to conceal your identity. The downside of

sharing IP addresses is the off chance that another user has breached a website's terms of service. If that user's actions resulted in the IP address getting blocked, you will also be blocked by the service or website when it's your turn to use the IP address. Using a VPN service with a lot of IP addresses minimizes the likelihood of this happening.

Server count and the number of server locations: Both of these can affect your online speeds. For faster download speeds, you want to use a server that's geographically close to you and not overloaded by too many VPN users.

Country locations: This refers to the locations where the VPN servers are, not the locations where the VPN works. You may want to select a specific country to unblock geo-restricted content or to have a server network physically close to you for faster speeds.

Static IP available: When you log in to a VPN service, it usually replaces your IP address with one from its VPN servers, randomly assigning you a different IP address each time. Sometimes it's advantageous to use the same IP address each time, which is called a static or dedicated IP address. This is often an upgrade to your monthly subscription.

What devices do you need a VPN for?

Best VPN's Device Compatibility

[NordVPN »](#)
Windows
Mac
Linux
iOS
Android
Router

Number of devices supported: VPN subscriptions typically allow for multiple simultaneous connections, which is necessary if you want to connect more than one device to at the same time. This limit only includes devices that are currently connected to the VPN, not the total number that the VPN is installed on. Some VPN providers also support routers. A router counts as one device and secures the data of every device connected to your home Wi-Fi network. This is especially helpful when you have baby monitors and other Wi-Fi-enabled devices that can't download

apps.

Smartphones and tablets: Most VPN services have iOS and Android apps that you can download directly on your phone or tablet. A few also have apps for Blackberry and Windows mobile devices.

Computers: Support for Windows and Mac operating systems is universal, and support for Linux is common, making it easy to install a VPN on most laptops. A few VPN providers even have apps for Chromebooks. An alternative to a desktop app is a browser extension, though the security features of these can be different from the main desktop app. Browser extensions for Chrome and Firefox are the most common.

What do you want to use a VPN for?

Surfshark »

Netflix

disney+

Hulu

Amazon Prime

View Plans »

Special Offer: Get TWO additional months FREE on Two-Year Plans

Streaming: Not all VPNs work with all streaming services, so be sure to check if the VPN you are considering is compatible if streaming is important to you. For more information on streaming services, including info on the best live and on-demand companies, see our Streaming Services guide.

File sharing: Sharing large files, performing large cloud backups, or updating multiplayer games are some of the reasons you may want to use a P2P network or torrenting client. Most of the best VPNs support legal P2P applications.

How much does a VPN service cost?

Price Comparison of VPN Plans

ExpressVPN »

| Monthly Plan $12.95/Month |
| Annual Plan $8.32/Month |
| Dedicated IP Fee Not Applicable |
| Trial Period Not Applicable |
| Money-Back Guarantee 30 Days |

NordVPN »

| Monthly Plan $11.95/Month |
| Annual Plan $4.92/Month |
| Dedicated IP Fee $5.83/Month |
| Trial Period Not Applicable |
| Money-Back Guarantee 30 Days |

Surfshark »

| Monthly Plan $12.95/Month |
| Annual Plan Not Offered |
| Dedicated IP Fee None |
| Trial Period 7 Days |
| Money-Back Guarantee 30 Days |

Private Internet Access »

| Monthly Plan $9.95/Month |
| Annual Plan $3.33/Month |
| Dedicated IP Fee $5.00/Month |
| Trial Period 7 Days |
| Money-Back Guarantee 30 Days |

IPVanish »

| Monthly Plan $10.99/Month |
| Annual Plan $7.50/Month ($3.75/mo. For the first year) |

| Dedicated IP Fee Not Applicable |
| Trial Period Not Applicable |
| Money-Back Guarantee 30 Days on Annual Plan |

Company	Monthly Plan	Annual Plan	Dedicated IP Fee	Trial Period	Money-Back Guarantee
ExpressVPN »	$12.95/Month	$8.32/Month	Not Applicable	Not Applicable	30 Days
NordVPN »	$11.95/Month	$4.92/Month	$5.83/Month	Not Applicable	30 Days
Surfshark »	$12.95/Month	Not Offered	None	7 Days	30 Days
Private Internet Access »	$9.95/Month	$3.33/Month	$5.00/Month	7 Days	30 Days
IPVanish »	$10.99/Month	$7.50/Month ($3.75/mo. For the first year)	Not Applicable	Not Applicable	30 Days on Annual Plan

The average cost of a month-to-month VPN service in our rating is just over $11, with prices ranging from $10 a month to about $15 a month. You can significantly lower your monthly cost to around $3 by signing up for an annual plan or as low as $2 per month by signing up for a multiyear plan, which generally is billed upfront.

Some VPNs don't cost anything, but you may want to be wary of these. "Many VPN apps are free because they sell advertising within the app, or because they share your information with (or redirect your traffic through) third parties," states the FTC. A separate study of VPN apps with free plans available for Android devices found that 75% of the apps used third-party tracking, and more than 38% contained some type of malware. There are a few dependable companies with free plans, which we name in our rating of the Best Free VPNs of 2022.

How To Get and Set Up a VPN

Before getting a VPN, ask yourself the following questions:

1. **Why do I need a VPN?** Consider how you interact with the internet. What type of online activity do you engage in? Identify how you use the internet and make a list of your most common online activities. Once you take stock of your digital behaviors, you will know exactly what to look for in a VPN and how it can help you.
2. **Consider your options.** With your list of common online activities, you will now be able to search for a VPN that can meet your specific needs. And while researching VPNs can be overwhelming, our ratings have done the work for you. Read some of the reviews of our Best VPNs of 2022 and find a few

options of VPN providers that are offering the features and compatibility that is right for you.

3. **Determine your budget.** Now that you have some options of VPN services to pick from, figure out which companies are within your price range. Keep in mind that many of these companies offer free trials and money-back guarantees. Some even offer free VPNs with limitations, such as data caps. These are great options to test out the VPNs you're interested in risk-free. If you test out a VPN and find it works for you, remember that you can save a lot of money by opting for an annual subscription instead of a month-to-month plan.

4. **Install your VPN software.** Once you've found a VPN that is right for you, purchase your VPN plan and set it up. You don't have to be tech-savvy to use a VPN – below we give you advice on how to set up your VPN.

To install a VPN, first create an account with your VPN provider. Many VPN services accept numerous forms of payment, and some even include Bitcoin, to help support your online anonymity.

When you have your account set up, you will have a few options of how you want to use the VPN on your devices. This decision will depend on the compatibility of your VPN and the number of simultaneously connected devices your VPN provider offers. In general, you will need to download the VPN app on each device you plan to use it on. Many VPN services also have VPN browser extensions that you can use instead of downloading a VPN app.

If your VPN service offers a limited number of connections, you may want to consider installing the VPN on your router. This covers all devices connected to the internet through your router, but it comes at the cost of slowing down your overall internet speed. Installing a VPN on your router is also slightly more complicated than using a VPN with devices such as laptops and tablets, but it is still a manageable process.

Best VPN Coupons and Discount Codes

Learn More

Still looking for more information about VPNs or trying to find the best VPN for you? Explore the directory below to learn more about these services.

Other Ratings from 360 Reviews

Our 360 Methodology for Evaluating VPN Services

Why You Can Trust Us: 26 VPNs Researched

At U.S. News & World Report, we rank the Best Hospitals, Best Colleges, and Best Cars to guide readers through some of life's most complicated decisions. Our 360 Reviews team draws on this same unbiased approach to rate the products that you use every day. To build our Best VPNs of 2022 rating, we researched more than 26

VPNs and analyzed 23 reviews. Our 360 Reviews team does not take samples, gifts, or loans of products or services we review. All sample products provided for review are donated after review. In addition, we maintain a separate business team that has no influence over our methodology or recommendations.

The following describes our 360 approach to researching and analyzing VPNs to guide prospective consumers.

1. We researched the companies and products people care most about.

U.S. News analyzed and compared a variety of publicly available data, including internet search data, to determine which VPN companies Americans are most interested in. We found 20 companies that stand out in terms of volume of searches and research among consumers, as well as across the different rating sources.

We then compared the available VPNs provided by our top VPN companies across several criteria, including monthly fees, compatibility with common systems, and technical capabilities such as type of protocols, number of servers, and IP addresses. Research shows that these are the most important criteria for people shopping for a VPN. We then narrowed the list down to the twelve best VPNs.

2. We created objective 360 Overall Ratings based on an analysis of third-party reviews.

U.S. News' 360 Reviews team applied an unbiased methodology that includes opinions from professional reviews as well as consumer reviews.

Our scoring methodology is based on a composite analysis of the ratings and reviews published by credible third-party professional and consumer review sources. The ratings are not based on personal opinions or experiences of U.S. News. To calculate the ratings:

(a) We compiled two types of third-party ratings and reviews:

- *Professional Ratings and Reviews.* Many independent VPN evaluating sources have published their assessments of VPN companies and their products online. We consider several of these third-party reviews to be reputable and well-researched. However, professional reviewers often make recommendations that contradict one another. Rather than relying on a single source, U.S. News believes consumers benefit most when these opinions and recommendations are considered and analyzed collectively with an objective, consensus-based methodology.
- *Consumer Ratings and Reviews.* U.S. News also reviewed published consumer ratings and reviews of VPN providers. Sources with a sufficient number of quality consumer ratings and reviews were included in our scoring model.

Please note that not all professional and consumer rating sources met our criteria for objectivity. Therefore, some sources were excluded from our model.

(b) We standardized the inputs to create a common scale.

The third-party review source data were collected in a variety of forms, including ratings, recommendations, and accolades. Before including each third-party data point into our scoring equation, we had to standardize it so that it could be compared accurately with data points from other review sources. We used the scoring methodology described below to convert these systems to a comparable scale.

The 360 scoring process first converted each third-party rating into a common 0 to 5 scale. To balance the distribution of scores within each source's scale, we used a standard deviation (or Z-Score) calculation to determine how each company's score compared to the source's mean score. We then used the Z-Score to create a standardized U.S. News score using the method outlined below:

- Calculating the Z-Score: The Z-Score represents a data point's relation to the mean measurement of the data set. The Z-Score is negative when the data point is below the mean and positive when it's above the mean; a Z-Score of 0 means it's equal to the mean. To determine the Z-Score for each third-party rating of a company, we calculated the mean of the ratings across all companies evaluated by that third-party source. We then subtracted the mean from the company's rating and divided it by the standard deviation to produce the Z-Score.
- Calculating the T-Score: We used a T-Score calculation to convert the Z-Score to a 0-100 scale by multiplying the Z-Score by 10. To ensure that the mean was equal across all data points, we added our desired scoring mean (between 0 and 10) to the T-Score to create an adjusted T-Score.
- Calculating the common-scale rating: We divided the adjusted T-Score, which is on a 100-point scale, by 20 to convert the third-party rating to a common 0-5 point system.

(c) We calculated the 360 Overall Score based on a weighted-average model.

We assigned "source weights" to each source used in the consensus scoring model based on our assessment of how much the source is trusted and recognized by consumers and how much its published review process indicates that it is both comprehensive and editorially independent. The source weights are assigned on a 1-5 scale. Any source with an assigned weight less than two was excluded from the consensus scoring model.

Finally, we combined the converted third-party data points using a weighted average formula based on source weight. This formula calculated the consensus score for each product, which we call the 360 Overall Rating.

U.S. News 360 Reviews takes an unbiased approach to our recommendations. When you use our links to buy products, we may earn a commission but that in no way affects our editorial independence.

Browser Fingerprinting Protection: How to Stay Private

Sven Taylor

In this guide we cover all aspects of browser fingerprinting and device fingerprinting in 2022. In addition to explaining what exactly this is, we'll also show you how to protect yourself against these threats.

Many people use VPN services to hide their IP address and location – but there is another way you can be identified and tracked online. That is through browser fingerprinting.

Whenever you go online, your computer or device provides the sites you visit with **highly specific information** about your operating system, settings, and even hardware. The use of this information to identify and track you online is known as device or browser fingerprinting.

As browsers become increasingly entwined with the operating system, many unique details and preferences can be exposed through your browser. The sum total of these outputs can be used to render a unique "fingerprint" for tracking and identification purposes.

Your browser fingerprint can reflect:

- the User agent header
- the Accept header
- the Connection header
- the Encoding header
- the Language header
- the list of plugins
- the platform
- the cookies preferences (allowed or not)
- the Do Not Track preferences (yes, no or not communicated)
- the timezone
- the screen resolution and its color depth
- the use of local storage
- the use of session storage
- a picture rendered with the HTML Canvas element
- a picture rendered with WebGL
- the presence of AdBlock
- the list of fonts

Is browser fingerprinting accurate?

Some researchers have found this method of identification to be [extremely effective](#).

Why is this being done?

Browser fingerprinting is just another tool to identify and track people as they browse the web. There are many different entities – both corporate and government – that are monitoring internet activity, and they all have different reasons for doing so. Advertisers and marketers find this technique useful to acquire more data on users, which in turn leads to more advertising revenue.

Some websites use browser fingerprinting to detect potential fraud, such as banks or dating websites, so it's not always nefarious.

Surveillance agencies could also use this to identify people who are employing other privacy measures to cloak their IP address and location, such as with VPN services or the Tor (onion) network.

Browser fingerprinting test websites

One good test website to see all of the information that is being revealed by your browser is ipleak.net.

With ipleak.net, you will want to scroll down to the "**Geek Details**" section where you will be able to see:

- Detected information
- System information
- Screen information
- Plugins information
- Mime-Types information
- HTTP Request Headers

There are also a few websites that reveal browser data and also assess a "uniqueness" score based on your variables in comparison to their database of browsers.

- amiunique.org is another good resource. It is open source and provides more information and updated fingerprinting techniques, including webGL and canvas.
- **Cover Your Tracks** is run by the Electronic Frontier Foundation. You can learn more here.

Cover Your Tracks is the updated version of a project the EFF has been working on for many years. It gives you a pretty good picture of how susceptible your browser is to finger printing.

How to mitigate your browser fingerprint

Before we jump into potential solutions, it's important to note that implementing browser fingerprinting protection methods **may break some websites**. Be sure to research these different options carefully before adjusting your browser settings.

Another consideration is your **threat model**. How much privacy do you need or want? The answer to that question will be

different for every user.

Lastly, I use the word "mitigate" rather than "solve" because browser fingerprinting is a very complex and evolving issue. For example, a new study revealed that there's nothing you can do to mitigate some fingerprinting attacks on smartphones (discussed more below).

Here are some good ways to mitigate your browser fingerprint:

1. Browser modifications and tweaks

Depending on the browser you are using, you might have some different options for tweaks and modifications to mitigate browser fingerprinting. Below we'll discuss various Firefox and Brave browsers, which are both secure and private browsers.

Brave browser fingerprinting

Although it is based on Chromium, the Brave Browser may be a good option for those wanting a simple, privacy-focused browser that blocks tracking by default and still supports Chrome extensions. Brave allows you to enable fingerprinting protection, which is under the Brave **Shields** settings:

See also this article on Github discussing different aspects of fingerprinting protection in Brave.

Firefox browser fingerprinting

Firefox is a good browser for privacy and security, and it can also be modified and hardened for your unique needs. (For an overview of Firefox privacy tweaks, see the Firefox privacy guide.) The first thing you need to do is type **about:config** into the URL bar of Firefox, hit enter, then agree to "accept the risk" and make the following changes:

- **privacy.resistFingerprinting** (change to **true**) – Changing this value to **true** will offer some basic protection, but it's far from a complete solution. The privacy.resistFingerprinting preference was added to Firefox as part of the Tor Uplift project and it continues to be improved.
- **webgl.disabled** (change to **true**) – WebGL is another tricky issue for privacy and security. Disabling this preference is generally a good idea – see some of the issues with WebGL here.
- **media.peerconnection.enabled** (change to **false**) – Disabling WebRTC is a good idea since this can reveal your true IP address, even when you are using a good VPN service. See the WebRTC leak guide for more details and how to disable WebRTC in other browsers.
- **geo.enabled** (change to **false**) – This disables geolocation tracking.
- **privacy.firstparty.isolate** (change to **true**) – This is another great update from the Tor Uplift project that isolates cookies to the first party domain.

Note: This is just a brief overview of changes that improve your privacy and help to mitigate your browser fingerprint. Nonetheless, there are many different factors that go into fingerprinting and you may still have a unique fingerprint even with these changes.

Firefox with the ghacks user.js file

Another great option is to run Firefox with a unique user.js file, such as the ghacks user.js. This is a custom Firefox configuration file that has been modified for more privacy and security. I like this option because it can save lots of time with setup and is regularly updated and improved. See the Wiki page for an overview and setup instructions.

When I tested a fresh install of Firefox with the ghacks user.js file, amiunique.org showed my browser fingerprint as as not unique.

2. Browser extensions and add-ons to minimize or spoof your fingerprint

There are a number of different browser extensions and add-ons that you may find useful. With that being said here are a few

things to remember:

1. Be careful with third-party extensions, which could potentially undermine your privacy and security.
2. Be mindful that using extensions may make your browser fingerprint more unique (many factors).

Now that we've gotten those disclaimers out of the way, let's examine some browser add-ons that may be useful:

Firefox browser:

- Canvasblocker by kkapsner – Protects against canvas fingerprinting methods (source on GitHub)
- Trace by AbsoluteDouble – Protects against various fingerprinting methods (source on GitHub)
- Chameleon by sereneblue – Allows you to spoof user agent values (source on GitHub)

There are many other Firefox add-ons you may want to consider as well, which are discussed in the Firefox privacy guide. Some of these add-ons are also available for Chromium-based browsers, such as Brave.

Some people recommend spoofing different user agents through a browser extension, while others suggest this is a bad idea because it might make you more "unique". Of course, there are many factors to consider, but adding noise to your fingerprint may not be a bad strategy.

For example, with Chameleon, you can cycle through different user agents at various time intervals.

Now let's look at another option for modifying your browser fingerprint: the use of virtual machines.

3. Virtual machines

You can also consider running different virtual machines, which can utilize different operating systems on your host computer. VirtualBox is FOSS and offers an easy way to run different Linux VMs for more privacy and security. There are many different video tutorials online, depending on your operating system and the VM OS you are looking to use.

Virtual machines offer numerous advantages in terms of privacy and security, while also protecting your host machine. For privacy, VMs allow you to easily spoof different operating systems and also chain VPN services, as explained in the multi-hop VPN guide. This also helps keep your host machine secure by isolating a virtual environment. If the VM were to be compromised, simply delete it and create a new one. You can also use different VMs for different purposes.

4. Tor Browser

Another option is to use the Tor browser, which is simply a hardened and protected version of Firefox. It includes numerous privacy and security modifications that are built into the default version:

- HTTPS Everywhere
- NoScript
- Anti-tracking features
- Canvas image extraction blocked
- WebGL blocked
- Operating system cloaking (shows as Windows 7 for all users)

- Timezone and language preferences blocked

The key here is to **use the default version** (the developers do not recommend adding any plugins or extensions because this could compromise the browser's effectiveness).

You can get the latest version of the **Tor browser here**.

The default version of the Tor browser is configured to run with the Tor (anonymous/onion) network. While the Tor network does have added benefits in terms of privacy, it also has a number of disadvantages:

- Your internet speed will be reduced to around 2 Mbps, making streaming videos or music nearly impossible
- Tor only encrypts traffic through the browser, rather than encrypting all traffic on your operating system like a VPN
- Tor is vulnerable to IP leaks, especially with Windows
- Tor is not safe to use when torrenting (see the Best VPNs for Torrenting guide)
- Tor was created by the US government and is still funded largely by US government grants
- Some consider Tor to be compromised

Ultimately, like all privacy tools, Tor has both pros and cons.

Note: You can also first connect to a VPN and then load the Tor browser as normal with the VPN running in the background. This will hide your real IP address from malicious Tor nodes and give you an extra layer of protection.

5. Don't expect much privacy on a smart phones

As we've covered before, most "smart" devices are data collection tools for various entities.

Smart phones are especially vulnerable to browser fingerprinting. A team of researchers at Cambridge published a paper highlighting how smartphones can be fingerprinted using internal sensors – and there's nothing the user can do about it.

The paper delves into the technical details, but here's a brief overview of their findings:

- The attack can be launched by any website you visit or any app you use on a vulnerable device without requiring any explicit confirmation or consent from you.
- The attack takes less than one second to generate a fingerprint.
- The attack can generate a globally unique fingerprint for iOS devices.
- The calibration fingerprint never changes, even after a factory reset.
- The attack provides an effective means to track you as you browse across the web and move between apps on your phone.

Aside from the sensor issue, there are many other reasons for avoiding smart phones if you expect privacy. See our article on controlling communication channels for more info on this topic.

Use a good VPN service

Although a VPN alone won't protect you against browser fingerprinting, it is a very important privacy tool to hide your IP address, hide your location, and keep your data secure.

If you're not using a good VPN, your internet provider can easily monitor all your online activity by recording your DNS requests. In many countries, such as the UK and Australia, this is mandatory. Internet providers in the US can also monitor and record their users, and since March 2017, they can also sell this information to third parties (advertisers).

An interesting report from the Federal Trade Commission in the US highlighted how **all major internet providers are collecting vast amounts of private data** and sharing this data within a wide network of partners. See our article for more details:

Internet Service Providers are Logging EVERYTHING You Do Online

Going through all the hassle to protect yourself against browser fingerprinting may be a waste of time if you aren't using a good VPN that will encrypt your internet connection and hide your IP address and location. The best VPN services report discusses the top recommendations based on the latest results.

For those who are seeking a higher level of online anonymity, you can also use a multi-hop VPN, which will encrypt your traffic across more than one server (multiple hops) before exiting onto the regular internet.

As mentioned above, combining VPNs also adds additional privacy and security while distributing trust across different VPN providers.

Browser Fingerprinting FAQs

Below are some of the other questions we see regarding browser fingerprinting.

What do you mean by browser fingerprinting?

Browser fingerprinting is a method to identify and track you online based on numerous different variables, including your operating system, timezone, browser headers, plugins, cookie preferences, tracking preferences, screen resolution and more. By aggregating these browser variables, third parties can create a unique fingerprint of your browser so that you can be identified and tracked online.

Who uses browser fingerprinting?

Browser fingerprinting is used primarily by advertising agencies and data brokers. By creating a unique browser fingerprint, ad agencies and data brokers can track your activities as you browse different websites. Your browsing activity can then be linked to your unique browser fingerprint, which allows you be targeted with ads based on your online activities. Additionally, your activities and identity can be sold to third parties by data brokers and other ad-tech intermediaries.

Does a VPN prevent browser fingerprinting?

No, a VPN alone will not protect you against browser fingerprinting. While a VPN will hide your true ISP-assigned IP address and location, it will not protect you against browser fingerprinting, which is based on unique variables without your browser and operating system. To protect yourself against browser fingerprinting, you will need to modify the settings within your browser, as we describe above. However, you should still use a VPN to hide your IP address and location to better protect your online privacy.

Can you be tracked on private browsing?

Private browsing alone will not protect you from browser fingerprinting and it also won't hide your IP address or location. In essence, private browsing is not actually private. We explain why incognito/private browsing is not private and the steps you can take to actually have more privacy and security online with your browser.

Use browser fingerprinting protection in 2022

While browser fingerprinting may seem like a daunting issue to some, mitigating your browser fingerprint is relatively easy. For those seeking the highest levels of privacy and security, I'd recommend utilizing virtual machines and perhaps chaining different VPN services (using more than one VPN at the same time).

As a general rule of thumb, Firefox remains a great all-around browser after some modifications and configuration. The secure browsers guide also discusses various options, while the Firefox privacy modifications guide takes a deep-dive into tweaks, extensions, and custom configuration.

Another issue to consider, which was not mentioned in this guide, is using a good ad blocker. Ads today basically function as tracking – they record your browsing habits so you can be hit with targeted advertisements. A good add-on is **uBlock Origin**, but there are other recommendations in the ad blocker article and privacy tools guide.

Stay safe, secure, and private in 2022 and beyond. We're all being watched.

Search …   US   °F   GO PREMIUM

| Today | Hourly | 10 Day | Weekend | Monthly | Radar | More |

Vendor Privacy Practices and Opt Outs

In order to provide accurate weather data free of charge, we serve personalized ads on our sites and apps. As described in our Privacy Policy:

> We work with vendors for advertising purposes. These vendors use cookies and mobile advertising identifiers to direct and measure "personalized ads", which are tailored to your likely interests based on your activities across some of the other apps and websites you use. We work with analytics vendors that use data collection technologies to track, analyze, and report data about the use of our websites or apps and to analyze and optimize the performance of the websites or apps. We work with technology vendors to support our apps and websites; for transparency, we list those vendors below.

This page lists opt-out options provided by our vendors as well as links for you to find information about their privacy practices. We may use these vendors for all or some of our apps and websites, and may use different vendors in specific regions.

The opt-outs described below may be device- or browser-specific and may not be available for all devices. The scope of the opt-outs is determined by each vendor. For example, if you opt out on your mobile device, you may continue to receive personalized advertising on your desktop computer or other devices. If you choose to opt out, you will still see ads, but the ads will not be personalized ads.

This page is updated periodically to reflect the most up to date information related to our vendors.

To opt out of sales under the California Consumer Privacy Act, please visit our Privacy Settings page.

Industry Group Opt Outs

Some industry organizations offer centralized tools where you can opt out of the use of your data

by multiple vendors at once. For more information about Digital Advertising Alliance (DAA) and Network Advertising Initiative (NAI) opt-out tools to assist you in managing choices for participating companies that use cookies, visit the following sites:

The DAA's opt-out page The Digital Advertising Alliance of Canada's (DAAC's) opt-out page One of the EDAA's country-specific opt-out pages The NAI's opt-out page

Also, the DAA offers AppChoices, a separate choice tool for users to exercise control over the collection and use of data through mobile applications for personalized advertising and other related uses. To exercise choice for participating companies, you can install the DAA's AppChoices application on your mobile device. Visit here for more information on DAA's AppChoices tool.

Advertising Vendors

We work with advertising vendors that use data collection technologies to track usage behavior to deliver relevant content or ads on our or other websites or apps, and to analyze and report on content or ads which users see and interact with. Note: this list does not include the advertising vendors used by our advertisers.

33Across
- Privacy Policy
- Opt Out

Acuity / 140 Proof (US only)
- Privacy Policy
- Opt Out

AdForm (US Only)
- Privacy Policy
- Opt Out

Amazon
- Privacy Policy
- Opt Out

Apps Flyer
- Privacy Policy

Arts.ai (US only)
- Privacy Policy
- Opt Out

Beachfront Media (US only)

- Privacy Policy

- Opt Out

BounceX (US only)

- Privacy Policy

- Opt Out

Braze

- Privacy Policy

Burda-Forward (Germany only)

- Opt Out

- Data Protection

Celtra (US only)

- Privacy Policy

Claritas (US Only)

- Privacy Policy

- Opt Out

Connatix (US Only)

- Privacy Policy

- Opt Out

Criteo (US Only)

- Privacy Policy

- Opt Out

Disqo (US Only)

- Privacy Policy

- Opt Out

DoubleClick / Google AdX

- Privacy Policy

DoubleVerify

- Privacy Policy

Dynata (US Only)

- Privacy Policy

- Opt Out

Facebook (US Only)

- Privacy Policy

- Opt Out

Google Ad Manager 360

- Privacy Policy

- How Google uses information from sites or apps that use its services

- Opt out ("Ad Personalization") - Opt out ("My Google Activity")

Improve Digital (US only)

- Privacy Policy

- Opt Out

Index Exchange

- Privacy Policy

- Opt Out

Influential (US Only)

- Privacy Policy

- Opt Out

InMobi

- Privacy Policy

- Opt Out

Integral Ad Science (IAS) (US Only)

- Privacy Policy

IRI Worldwide (US only)

- Privacy Policy

Kargo

- Privacy Policy

- Opt Out

LiveRamp (US only)

- Privacy Policy

- Opt Out

Lotame (US Only)

- Privacy Policy

- Opt Out

Lucid (US only)

- Privacy Policy

- Opt Out

Magnite / Rubicon Project

- Privacy Policy

- Opt Out

Media.net

- Privacy Policy

- Opt Out

Millward Brown (US only)

- Privacy Policy

- Opt Out

MixPanel (US only)

- Privacy Policy

Nielsen (US only)

- Privacy Policy

- Opt Out

OneTag (US Only)

- Privacy Policy

- Opt Out

OpenX

- Privacy Policy

- Opt Out

Oracle Advertising / Moat

- Privacy Policy

Outbrain (Germany Only)

- Privacy Policy

- Opt Out

Pubmatic

- Privacy Policy

- Opt Out

RhythmOne / UnRuly (US only)

- Privacy Policy
- Opt Out

Sharethrough

- Privacy Policy

Smaato (US only)

- Privacy Policy
- Opt Out

SmartCommerce (US Only)

- Privacy Policy

Sonobi (US only)

- Privacy Policy
- Opt Out

SpotXchange (US only)

- Privacy Policy
- Opt Out

Taboola

- Privacy Policy
- Opt Out

Teads (US, non-EU countries)

- Privacy Policy

The MediaGrid

- Privacy Policy
- Opt Out

TripleLift (US Only)

- Privacy Policy

Upwave / Survata (US Only)

- Privacy Policy

Vdopia / Chocolate (US only)

- Privacy Policy
- Opt Out

Xandr / AppNexus

- Privacy Policy

- Opt Out

Yahoo / Verizon Media (US, Canada, Japan only)

- Privacy Policy

- Opt Out

Yield Mo (US, Canada, Australia only)

- Privacy Policy

- Opt Out

Analytics Vendors

We work with certain analytics vendors that use data collection technologies to track, analyze, and report data about the use of our websites or apps, and to analyze and optimize the performance of the websites or apps.

AGOF (Germany only)

- Privacy Policy

- Opt Out

Alchemer (US Only)

- Privacy Policy

Amplitude

- Privacy Policy

Apps Flyer

- Privacy Policy

Apptentive

- Privacy Policy

Braze

- Privacy Policy

Comscore

- Privacy Policy

Firebase

- Privacy Policy

InfOnline (Germany Only)

- Privacy Policy

- Opt Out

Instana

- Privacy Policy

IVW (Germany only)

- Privacy Policy

- Opt Out

JW Player

- Privacy Policy

Localytics

- Privacy Policy

Medallia (US Only)

- Privacy Policy

Piano (US Only)

- Privacy Policy

Taboola

- Privacy Policy

- Opt Out

UserZoom (US Only)

- Privacy Policy

Technology Vendors

We work with certain technology vendors that use data collection technologies to support the apps and websites. These vendors assist us with our business operations, with the provision of the apps and websites, or in delivering you the features and functionality that you have requested.

Akamai

Amazon Alexa

Apps Flyer

AWS (Amazon)

Confiant

Cybersource

Data Dog

DefineMedia

eSignature

Experian

Fastly

Google Play Store

IBM Cloud

IBM Cloudant

iOS App Store

JW Player

LoginRadius

Mapbox

MongoDB

Piano

Salesforce

TrustArc

Connect With Us

The Weather Company
An IBM Business

The Weather Channel

WEATHER UNDERGROUND

Feedback   Careers   Press Room   Advertise With Us   TV

Terms of Use | **Privacy Policy** | **Ad Choices** | **Accessibility Statement** | **Data Vendors**

Georgia®

We recognize our responsibility to use data and technology for good. Take control of your data.

Privacy Settings | **Review My Advertising Settings** | **Data Rights**

Powered by the   IBM **Cloud**

WIKIPEDIA

Google Chrome version history

Google Chrome is a freeware web browser developed by Google LLC. The development process is split into different "release channels," each working on a build in a separate stage of development. Chrome provides 4 channels: Stable, Beta, Dev, and Canary. On the stable builds, Chrome is updated every two to three weeks for minor releases and every four weeks for major releases.[1]

Contents

Versions

See also

Notes

References

External links

Versions

The following table summarizes the release history for the Google Chrome web browser.

	Discontinued		Extended Stable Channel (macOS and Windows)		Stable Channel		Beta Channel		Developer Channel		Canary Channel

Major version	Release date	Layout engine[r 1]	V8 engine[r 2]	Significant changes	Issues/Bugs
0.2.149	2008-09-02	WebKit 522	0.3	• First release[r 3]	
0.3.154	2008-10-29			• Improved plugin performance and reliability • Spell checking for input fields • Improved web proxy performance and reliability • Tab and window management updates	
0.4.154	2008-11-24	WebKit 525		• Bookmark manager with import and export support • Privacy section added to the application options • New blocked popup notification	
1.0.154	2008-12-11	WebKit 528		• First stable release	
2.0.172	2009-05-24	WebKit 530	0.4	• 35% faster JavaScript on the SunSpider benchmark • Mouse wheel support • Full-screen mode • Full-page zoom • Form auto-fill • Sort bookmarks by title • Tab docking to browser and desktop edges • Basic Greasemonkey support[r 4]	
3.0.195	2009-10-12	WebKit 532	1.2	• New "new tab" page for improved customization • 25% faster JavaScript • HTML5 video and audio tag support • Lightweight theme support[r 5]	
4.0.249	2010-01-25	WebKit 532.5	1.3	• Extensions • Bookmark synchronization • Enhanced developer tools • Improved HTML5 support • Performance improvements • Full ACID3 pass • HTTP byte range support • Experimental new anti-reflected-XSS feature called "XSS Auditor"[r 6]	
4.1.249	2010-03-17			• Translate infobar • New privacy features • Disabled XSS Auditor[r 7]	
5.0.375	2010-05-21	WebKit 533	2.1	• Browser preference synchronizing • Increased HTML5 support (Geolocation API, App Cache, web sockets, and file drag-and-drop)	
Major version	Release date	Layout engine[r 1]	V8 engine[r 2]	Significant changes	Issues/Bugs

Major version	Release date	Layout engine[r 1]	V8 engine[r 2]	Significant changes	Issues/Bugs
				- Revamped bookmark manager - Adobe Flash Player integrated[r 8][r 9] - First stable releases for macOS, 32 bit Linux, and 64 bit Linux[r 10]	
6.0.472	2010-09-02	WebKit 534.3	2.2	- Updated and more streamlined UI with simplified Omnibox - New tab page - Merged menu buttons - Form auto-fill - Expanded synchronization support to include extensions and auto-fill data - Support for WebM videos - Built-in PDF support (disabled by default)[r 11]	
7.0.517	2010-10-21	WebKit 534.7	2.3.11	- Implemented HTML5 parsing algorithm - File API - Directory upload via input tag - macOS version gained AppleScript support for UI automation[r 12] - Late binding enabled for SSL sockets: high priority SSL requests are now always sent to the server first. - New options for managing cookies - Updated New Tab page to enable featuring of web applications	
8.0.552	2010-12-02	WebKit 534.10	2.4.9	- Chrome Web Store - Built-in PDF viewer that works inside Chrome's sandbox for increased security - Expanded synchronization support to include web applications - Improved plug-in handling[r 13] - This release added "about:flags" to showcase experimental features such as Chrome Instant, side tabs on Windows, tabbed settings, Click to Play, background web applications, Remoting, disables outdated plug-ins, XSS Auditor, Cloud Print Proxy, GPU-accelerated compositing, WebGL support for the *canvas* element, and a "tab overview" mode (like Exposé) for macOS.	
9.0.597	2011-02-03	WebKit 534.13	2.5.9	- WebGL enabled by default - Adobe Flash sandboxing on Windows and Chrome Instant (a la Google Instant) option[r 14] - WebP support[r 15] - New flags: print preview, GPU-accelerated compositing, GPU-accelerated Canvas 2D, Google Native Client, CRX-less Web Apps,	
Major version	Release date	Layout engine[r 1]	V8 engine[r 2]	Significant changes	Issues/Bugs

Major version	Release date	Layout engine[r 1]	V8 engine[r 2]	Significant changes	Issues/Bugs
				Web page prerendering, experimental Extension APIs, disable hyperlink auditing	
10.0.648	2011-03-08	WebKit 534.16	3.0.12	■ Google Cloud Print sign-in interface enabled by default ■ Partially implemented sandboxing of the GPU process[r 16][r 17] ■ Faster JavaScript performance due to incorporation of Crankshaft, an improved compiler for V8[r 18] ■ Settings pages that open in a tab, rather than a dialog box ■ Malware reporting and disabling outdated plugins ■ Password sync ■ GPU accelerated video ■ Background WebApps ■ webNavigation extension API[r 19]	
11.0.696	2011-04-27	WebKit 534.24	3.1.8	■ HTML5 Speech Input API[r 20] ■ Updated icon[r 21]	
12.0.742	2011-06-07	WebKit 534.30	3.2.10	■ Hardware accelerated 3D CSS ■ New Safe Browsing protection against downloading malicious files ■ Ability to delete Flash cookies from inside Chrome[r 22] ■ Launch Apps by name from the Omnibox ■ Integrated Sync into new settings pages ■ Improved screen reader support ■ New warning when hitting Command-Q on Mac[r 22] ■ New flags: P2P API ■ Existing tab on foreground on open ■ Experimental new tab page ■ Add grouping to tab context menu ■ Run PPAPI Flash in the renderer process ■ Multiple profiles ■ Removed Google Gears ■ Print and Save buttons in the PDF viewer[r 23]	
13.0.782	2011-08-02	WebKit 535.1	3.3.10	■ Instant Pages (pre-rendering of Web pages)[r 24] ■ Native print interface and preview (Linux and Windows only) ■ Experimental new tab page ■ Experimental Restrict Instant To Search option	
14.0.835	2011-09-16		3.4.14	■ Native Client (NaCl) enabled for apps in the Chrome Web Store[r 25]	
Major version	Release date	Layout engine[r 1]	V8 engine[r 2]	Significant changes	Issues/Bugs

Major version	Release date	Layout engine[r 1]	V8 engine[r 2]	Significant changes	Issues/Bugs
				- Web Audio API - Additional macOS Lion feature support - Sync Encryption for all data - Print preview on Mac - Validation of HTTPS sites[r 26] - Experimental Web Request extension API - Experimental Content Settings extension API[r 27]	
15.0.874	2011-10-25	WebKit 535.2	3.5.10	- Faster print preview[r 28] - Redesigned new tab page on by default[r 28] - JavaScript fullscreen API enabled by default[r 28] - Inline installation of Chrome Web Store items by verified sites - Omnibox History synchronization[r 29] - Switched to FFmpeg native VP8 decoder[r 30] - Extensions integrated into settings pages - GPU Accelerated Canvas 2D disabled	
16.0.912	2011-12-13	WebKit 535.7	3.6.6	- Multiple profiles on by default[r 29] - Optional permissions in Chrome extensions, so the user can opt-in or opt-out of the optional permissions at installation time[r 31] - Experimental support for side tabs was removed.[r 32]	
17.0.963	2012-02-08	WebKit 535.11	3.7.12	- Updated Omnibox prerendering of pages[r 33] - Download scanning protection[r 33] - New extensions APIs[r 33] - Improved History tab - Removal of "+" symbol from the "new tab" button - Limited support for changing user agent strings - Adjustable margins in print preview[r 34] - Search engine synchronization[r 35] - Disabled GAIA profile info[r 36]	
18.0.1025	2012-03-28 2012-06-27 (Android ARM) 2012-09-26 (18.0.1026, Android x86)	WebKit 535.19	3.8.9	- Hardware-accelerated Canvas2D graphics[r 37] - WebGL without the need of 3D graphics hardware through the software rasterizer SwiftShader[r 37] - Brighter "new tab" button[r 38]	
Major version	Release date	Layout engine[r 1]	V8 engine[r 2]	Significant changes	Issues/Bugs

Major version	Release date	Layout engine[r 1]	V8 engine[r 2]	Significant changes	Issues/Bugs
19.0.1084	2012-05-15 2012-06-28 (iOS)	WebKit 536.5	3.9.24	■ Access tabs between devices[r 39] ■ Reorganized and searchable settings interface ■ Better spell check by using the Google search engine spell checker ■ Web Store link to the bottom of New Tab page ■ Experimental JavaScript Harmony (ECMAScript 6) support[r 40] ■ Experimental Web Intents API[r 41]	
20.0.1132	2012-06-26	WebKit 536.10	3.10.6	■ Experimental touch friendly user interface adjustments. Context menus have extra vertical padding between items.[r 42] ■ New tab button is bigger and wider	
21.0.1180	2012-07-31 2012-08-22 (iOS)	WebKit 537.1	3.11.10	■ Media Stream API (getUserMedia) enabled by default. (E.g. webcam access via JavaScript.)[r 43] ■ Gamepad API prototype available by default. ■ Support for (pointer) and (hover) CSS media queries so sites can optimize their user interface for touch when touch-screen support is available. ■ HTML5 audio/video and WebAudio now support 24-bit PCM wave files 　■ Note: This is the last version of Chrome that will run on Mac OS X 10.5.8 Leopard. (undocumented)	
22.0.1229	2012-09-25	WebKit 537.4	3.12.19	■ New-style packaged apps are enabled by default. ■ New menu icon, replacing the wrench icon ■ Support for TLS 1.1[r 44][r 45] ■ Support for color management ICC v2 profiles by default[r 46]	
23.0.1271	2012-11-06 2012-11-28 (iOS)	WebKit 537.11	3.13.7	■ Do Not Track preference[r 47] ■ Hardware video acceleration with 25% more efficient power consumption in some scenarios ■ Manager for site permission control ■ New icon for Chrome Web Store when opening new tab ■ PPAPI Flash Player (or Pepper-based Flash Player) replaced the NPAPI Flash Player on Mac also[r 48]	
24.0.1312	2013-01-10	WebKit 537.17	3.14.5	■ Support for MathML[r 49] ■ The HTML5 datalist element now supports suggesting a date and	
Major version	Release date	Layout engine[r 1]	V8 engine[r 2]	Significant changes	Issues/Bugs

Major version	Release date	Layout engine[r 1]	V8 engine[r 2]	Significant changes	Issues/Bugs
				time[r 49] ■ Experimental support for CSS custom filters[r 49][r 50]	
25.0.1364	2013-02-21 2013-02-27 (Android) 2013-03-04 (iOS)	WebKit 537.22	3.15.11	■ Support for Opus audio ■ Support for VP9 video[r 51] ■ Silent installs of external extensions are now disabled by default.[r 52] ■ Web Speech API[r 53] ■ Encrypted omnibox search (https)[r 54] ■ Native Client on ARM ■ Disabled MathML support for the time being[r 55] Android version (update from 18): ■ Newer V8 JavaScript engine ■ Audio now continues to play while Chrome is in the background ■ Support for pausing audio in Chrome when phone is in use	
26.0.1410	2013-03-26 2013-04-03 (Android) 2013-04-09 (iOS)	WebKit 537.31	3.16.14	■ Improved spell checker (grammar and homonym checking)[r 56] ■ Desktop shortcuts for multiple users (profiles) on Windows[r 56] ■ Asynchronous DNS resolver on Mac and Linux[r 56] Android version:[r 57] ■ Autofill and password sync ■ Performance and stability improvements	
27.0.1453	2013-05-21 2013-05-22 (Android) 2013-06-03 (iOS)	WebKit 537.36	3.17.6	■ Resource handling optimized for faster page loads[r 58] ■ Improved Omnibox predictions and spelling correction[r 58] ■ syncFileSystem API for Google Drive data synchronization[r 58] ■ Stop packaging Manifest version 1.0 extensions[r 59] Android version:[r 60] ■ Fullscreen on phones (scrolling down the page makes the toolbar disappear) ■ Simpler searching (the query stays visible in the omnibox, making it easier to edit) ■ Client-side certificate support ■ Tab history on tablets ■ "A ton of stability and performance fixes"	
Major version	Release date	Layout engine[r 1]	V8 engine[r 2]	Significant changes	Issues/Bugs

Major version	Release date	Layout engine[r 1]	V8 engine[r 2]	Significant changes	Issues/Bugs
28.0.1500	2013-06-17 (Linux) 2013-07-09 (macOS and Windows) 2013-07-10 (Android) 2013-07-17 (iOS)	Blink 28 (except iOS)	3.18.5	▪ Replaced layout engine with Blink, a fork of WebKit[r 61][r 62][r 63] on all platforms besides iOS ▪ Faster page loads with the new Blink threaded HTML parser[r 64] ▪ Rich Notifications and Notification Center (HTML-based notifications deprecated)[r 65] ▪ Major improvements to the asm.js benchmark performances[r 64] ▪ Support for the CSS :unresolved pseudoclass for Custom Elements[r 64] ▪ Support for the CSS @supports conditional blocks to test for property:value pairs[r 64] Android version: ▪ Fullscreen API support (fullscreen browsing on tablets)[r 64] ▪ Experimental WebGL, Web Audio, WebRTC support behind flags[r 64] ▪ Built-in translation[r 66] iOS version: ▪ Improved interoperability with many other Google Apps[r 67] ▪ Voice Search enhancements[r 67] ▪ Fullscreen for iPad[r 67] ▪ Data usage savings (rolling out over time)[r 67] ▪ Access to browser history[r 67]	
29.0.1547	2013-08-20 (Linux, macOS, and Windows) 2013-08-21 (Android) 2013-09-12 (iOS)	Blink 29 (except iOS)	3.19.18	▪ Support for VP9 final ▪ Support for TLS 1.2 ▪ Preliminary QUIC support[r 68] ▪ Improved Omnibox suggestions based on the recency of visited sites ▪ Ability to reset user profile back to its original state ▪ New apps and extensions APIs (such as Native Messaging API for connecting Chrome with native applications installed on the same computer - an alternative to NPAPI[r 69]) Android version: ▪ WebRTC support[r 70] ▪ WebAudio support[r 70] ▪ Improved scrolling responsiveness[r 71] and visual indication when scrolling to the top or bottom of a page[r 70] ▪ Startup performance and stability	
Major version	Release date	Layout engine[r 1]	V8 engine[r 2]	Significant changes	Issues/Bugs

Major version	Release date	Layout engine[r 1]	V8 engine[r 2]	Significant changes	Issues/Bugs
				improvements[r 71] ■ New color picker user interface for web forms[r 70] ■ Support for Google's experimental data compression service (comparable to Opera Turbo) that lets Google servers quickly read and optimize a Web page for mobile devices, then transmit it to the smartphone using Google's SPDY network technology. ■ Rudimentary tab groups implemented iOS version: ■ Get back to Search Results faster ■ Data cost savings enhancements (rolled out incrementally) ■ Voice search pronoun support (e.g. queries like: "Who is the president of the United States?" followed by "Who is his wife?") ■ Improvements to Single Sign On with other Google Apps[r 72] ■ Support for WebP image format[r 73]	
30.0.1599	2013-09-18 (iOS) 2013-10-01 (Linux, macOS, and Windows) 2013-10-02 (Android)	Blink 30 (except iOS)	3.20.17	■ New image context menu item: "Search Google for this image" ■ New Chrome Apps APIs: webview.request, media gallery write support and downloads[r 74] ■ New platform features (both in desktop and mobile): support for the WebRTC Device Enumeration API, allowing users to change their microphones and/or camera on the fly without having to restart the WebRTC call, DevTools now supports CSS source maps, Chrome will now match the behavior of IE and not honor the Refresh header or tags when the URL to be refreshed to has a javascript: scheme[r 74] ■ Removal of "History Index" files, previously used to quickly provide address bar results based on visited pages' text.[2] Android version: ■ New gesture: swipe horizontally across the top toolbar to quickly switch tabs ■ New gesture: drag vertically down from the toolbar to enter into the tab switcher view ■ New gesture: drag down from the menu to open the menu and select wanted item without having to lift finger ■ WebGL is enabled by default on	
Major version	Release date	Layout engine[r 1]	V8 engine[r 2]	Significant changes	Issues/Bugs

Major version	Release date	Layout engine[r 1]	V8 engine[r 2]	Significant changes	Issues/Bugs
				high-end devices[r 74] ■ DeviceMotion (device acceleration and rotation rates) events[r 74] ■ Media Source Extension is enabled on Android 4.1+[r 74] ■ Two new experimental features behind a flag: Web Speech API (recognition) and the Vibration API[r 74] iOS version: ■ New look and feature enhancements for iOS7 ■ Improvements to Fullscreen behavior especially on iPad (iOS7 only) ■ New Settings UI ■ Maps and email links launch the Google Maps and Gmail apps (if installed) automatically. You can change your preference in Settings ■ Stability / security improvements and bug fixes[r 75]	
31.0.1650	2013-11-12 (Linux, macOS, and Windows) 2013-11-14 (Android) 2013-11-20 (iOS)	Blink 31 (except iOS)	3.21.18	■ Payment requestAutocomplete() on Chrome for Android, Windows, Chrome OS ■ PNaCl on desktop versions of Chrome ■ New Chrome Apps APIs: With URL handlers for apps, Chrome App developers can now specify URLs to be handled by a Chrome App. For example, a document link on a website could open a document editor Chrome App. This gives users more seamless entry points into their favorite Chrome Apps. ■ Directory access for Apps allows Chrome Apps to access and write to user-approved folders. This feature can be used to share files between a Chrome App and a native app. For example, a Chrome App code editor could modify files managed by a native Git client. ■ SCTP for WebRTC Data Channel allows P2P data transfers between browsers to be either best effort, reliable, or semi reliable, opening up use cases such as gaming. ■ Alpha channel support for WebM video enables transparency masking (a.k.a. green screen effects) in WebM videos. ■ Speech recognition with the JavaScript Web Speech API is now supported on Chrome for Android. ■ window.devicePixelRatio now takes full-page zoom (but not pinch zoom) into account	
Major version	Release date	Layout engine[r 1]	V8 engine[r 2]	Significant changes	Issues/Bugs

Major version	Release date	Layout engine[r 1]	V8 engine[r 2]	Significant changes	Issues/Bugs
				■ Support for { alpha: false } in getContext('2d') lets you create an opaque canvas. This is similar to existing WebGL functionality and can improve the rendering performance of your app. ■ The Media Source API has been unprefixed and is now supported on Chrome for Android. It allows JavaScript to generate media streams for playback, addressing use cases like adaptive streaming and time shifting live streams. ■ 2D canvas now supports the "ellipse" method. ■ Support for several Mutation Events has been removed. Consider using MutationObserver instead.[r 76] iOS version: ■ Fast form completion with Autofill ■ Long press on an image to search for related images ■ Stability / security improvements and bug fixes[r 75]	

32.0.1700	2014-01-14 (Linux, macOS, and Windows) 2014-01-15 (Android) 2014-01-27 (iOS)	Blink 32 (except iOS)	3.22.24	■ Tab indicators for sound, webcam and casting
				■ A different look for Win8 Metro mode
				■ Automatically blocking malware files
				■ A number of new apps/extension APIs
				■ Various under-the-hood changes for stability and performance
				
				Android version:
				
				■ Add web page shortcuts right to your home screen more easily from the menu
				■ Reduce data usage in Chrome up to 50%. Visit Settings > Bandwidth management > Reduce data usage to enable.[r 77]
				
				iOS version:
				
				■ Translate
				  ■ When you come across a page written in a language that you don't understand, just look for the translation bar. One tap and the page is quickly translated for you.
				■ Reduce Data Usage
				  ■ Reduce your data usage by up to 50%. Enable this feature and view your savings: Settings > Bandwidth > Reduce Data Usage.	

Major version	Release date	Layout engine[r 1]	V8 engine[r 2]	Significant changes	Issues/Bugs

Major version	Release date	Layout engine[r 1]	V8 engine[r 2]	Significant changes	Issues/Bugs
				- New Tab Page update to make searching faster and easier - This feature is being rolled out and will be available to all users over time, beginning on iPhone.	
33.0.1750	2014-02-18 (iOS) 2014-02-20 (Linux, macOS, and Windows) 2014-02-26 (Android)	Blink 33 (except iOS)	3.23.17	- Custom Elements[r 78] - Ogg Opus in MSE and <video>[r 78] - Page Visibility API[r 78] - VTTCue [r 78] - Web Speech API (synthesis)[r 78] - Font-kerning[r 78] - requestAutocomplete()[r 78] - Speech Synthesis[r 78] Android version: - Download progress notification for file downloads using the Chrome network stack[r 79] - Updated help and feedback UI[r 79] - Support for <datalist> tag[r 79] iOS version: - Stability and security updates[r 75]	
34.0.1847	2014-04-02 (Android) 2014-04-08 (Linux, macOS, and Windows) 2014-04-29 (iOS)	Blink 34 (except iOS)	3.24.35	- Responsive Images and Unprefixed Web Audio - Import supervised users onto new computers - A different look for Windows 8 Metro mode - A number of new apps/extension APIs - New scroll bar look - Ignores autocomplete="off" on password input fields - Final version to not require SSE2[r 80] Android version: - Battery usage optimizations iOS version: - Updated tour when you start Chrome for the first time - Support for autocomplete in the omnibox for right to left languages	
35.0.1916	2014-05-20 (Android) 2014-05-20 (Linux, macOS, and Windows) 2014-05-28 (iOS)	Blink 35 (except iOS)	3.25.28	- More developer control over touch input - New JavaScript features - Unprefixed Shadow DOM v0 - A number of new apps/extension APIs	
Major version	Release date	Layout engine[r 1]	V8 engine[r 2]	Significant changes	Issues/Bugs

Major version	Release date	Layout engine[r 1]	V8 engine[r 2]	Significant changes	Issues/Bugs
				- Opus updated to version v1.1 **Android version:** - Undo Tab Close - Fullscreen video with Subtitles and HTML5 controls - Support for some multi-window devices **iOS version:** - Added right-to-left support to the omnibox for Arabic and Hebrew - See your search term in the omnibox, instead of the long search query URL - Easily refine your search queries and view more results on the search results page - Stability improvements and bug fixes[r 75] **Linux version:** - Switched graphics interface backend from GTK+ to Aura	
36.0.1985	2014-07-15 (iOS) 2014-07-16 (Linux, macOS, and Windows) 2014-07-16 (Android)	Blink 36 (except iOS)	3.26.31	- Rich Notifications Improvements - An Updated Incognito / Guest NTP design - The addition of a Browser crash recovery bubble - Multiple stability and performance improvements[r 81] **Android version:** - Improved text rendering on non-mobile optimized sites - Doodles return to the new tab page[r 82] **iOS version:** - Allows mobile sites that have added Cast support to work with your Cast-enabled device - Stability improvements and bug fixes[r 83] **Linux version:** - Chrome App Launcher[r 81]	
37.0.2062	2014-08-26 (Linux, macOS, and Windows) 2014-09-03 (Android) 2014-09-22 (iOS)	Blink 37 (except iOS)	3.27.34	- DirectWrite support on Windows for improved font rendering - A number of new apps/extension APIs - Discarded "Archived History" file previously used to store browsing	
Major version	**Release date**	**Layout engine[r 1]**	**V8 engine[r 2]**	**Significant changes**	**Issues/Bugs**

Major version	Release date	Layout engine[r 1]	V8 engine[r 2]	Significant changes	Issues/Bugs
				history for longer than 90 days.[3][4] ▪ Multiple stability and performance improvements[r 84] ▪ Removal of the showModalDialog API, breaking several enterprise web apps[r 85] Android version: ▪ Signing into Chrome signs you into your favorite Google sites ▪ Updated look and feel with elements of Material Design ▪ Multiple performance improvements and bug fixes[r 86] Windows version: ▪ 64-bit Windows support[r 87]	
38.0.2125	2014-10-07 (Linux, macOS, and Windows) 2014-10-07 (iOS) 2014-10-08 (Android)	Blink 38 (except iOS)	3.28.71	▪ A number of new apps/extension APIs ▪ Support for logging into sites using *FIDO U2F Security Key* (a USB or smartcard security token) as a factor in 2-factor authentication[r 88] ▪ Under-the-hood changes for stability and performance[r 89] Android version: ▪ Support for Battery Status and Screen orientation APIs ▪ Additional Material Design updates ▪ Bug fixes and performance improvements[r 90] iOS version: ▪ Better support for iPhone 6 and 6+ ▪ Download and open files in Google Drive ▪ Stability improvements and bug fixes ▪ Security fix[r 91]	
39.0.2171	2014-11-12 (Android) 2014-11-18 (Linux, macOS, and Windows) 2014-11-24 (iOS)	Blink 39 (except iOS)	3.29.88	▪ Removes SSL/TLS protocol version fallback to SSLv3 ▪ 64-bit support for Mac ▪ A number of new apps/extension APIs ▪ Under-the-hood changes for stability and performance[r 92] Android version: ▪ Number of bug fixes and performance improvements[r 93]	
Major version	Release date	Layout engine[r 1]	V8 engine[r 2]	Significant changes	Issues/Bugs

Major version	Release date	Layout engine[r 1]	V8 engine[r 2]	Significant changes	Issues/Bugs
				■ Experimental Reader Mode[r 94] can be enabled via chrome://flags, is not available for tablets in this version	
40.0.2214	2015-01-20 (iOS) 2015-01-21 (Linux, macOS, and Windows) 2015-01-21 (Android)	Blink 40 (except iOS)	3.30.33	■ Disabled SSLv3 support by default ■ The minimum SSL/TLS version can now be set through about:flags ■ Updated info dialog for Chrome app on Windows and Linux ■ A new clock behind/ahead error message[r 95] Android version: ■ Updated page info and content settings UI ■ Number of bug fixes and performance improvements[r 96] iOS version: ■ New look with Material Design bringing bold graphics, fluid motion, and tactile surfaces ■ iOS 8 optimizations and support for bigger phones ■ Support handoff from Chrome to your default browser on macOS ■ Stability improvements and bug fixes[r 97]	
41.0.2272	2015-03-03 (Linux, macOS, and Windows) 2015-03-11 (Android) 2015-03-16 (iOS)	Blink 41 (except iOS)	4.1.0	■ A number of new apps/extension APIs ■ Many under the hood changes for stability and performance[r 98] ■ Aero interface is disabled in Windows Vista Android version: ■ The ability to pull to reload at the top of most pages ■ A number of bug fixes and performance improvements[r 99]	
42.0.2311	2015-04-14 (Linux, macOS, and Windows) 2015-04-15 (Android) 2015-04-16 (iOS)	Blink 42 (except iOS)	4.2.77	■ Support for NPAPI plugins disabled by default ■ A number of new apps, extension and Web Platform APIs (including the Push API) ■ Many under the hood changes for stability and performance[r 100] ■ Add Bookmark is now redesigned. Android version: ■ Getting the latest updates from sites with notifications	
Major version	Release date	Layout engine[r 1]	V8 engine[r 2]	Significant changes	Issues/Bugs

Major version	Release date	Layout engine[r 1]	V8 engine[r 2]	Significant changes	Issues/Bugs
				- Adding your favorite sites to your homescreen is now even easier - Bug fixes and speedy performance improvements[r 101]	
43.0.2357	2015-05-19 (Linux, macOS, and Windows) 2015-05-27 (Android) 2015-06-01 (iOS)	Blink 43 (except iOS)	4.3.61	- Numerous bug fixes and security fixes[r 102] Android version: - Faster Checkout – Quickly and securely complete checkout forms with data from Google Wallet - Touch to Search – Learn more about words and phrases by touching them on your screen - Bug fixes and speedy performance improvements[r 103] - No longer supports Android 4.0 (Ice Cream Sandwich)[r 104][r 105]	
44.0.2403	2015-07-21 (Linux, macOS, and Windows) 2015-07-22 (iOS) 2015-07-29 (Android)	Blink 44 (except iOS)	4.4.63	- A number of new apps/extension APIs - Change in the loading page circle on Chrome tabs - Many under the hood changes for stability and performance[r 106] Android version: - Fixed a boatload of bugs and performance issues.[r 107] iOS version: - Swipe to navigate: swipe right or left to navigate backwards and forwards - Support for accessing Physical Web content from the Today view - Stability improvements and bug fixes[r 108]	
45.0.2454	2015-09-01 (Linux, macOS, and Windows) 2015-09-01 (Android) 2015-09-02 (iOS)	Blink 45 (except iOS)	4.5.103	- Support for NPAPI plugins permanently disabled - A number of fixes and improvements[r 109] Android version: - A number of fixes for a whole bunch of performance/stability/other issues.[r 110]	
46.0.2490	2015-10-13 (Linux, macOS, and Windows) 2015-10-14 (Android) 2015-10-22 (iOS)	Blink 46 (except iOS)	4.6.85	- Change in taskbar logo design - A number of fixes and improvements.[r 111] Android version: - Under the hood performance and	
Major version	Release date	Layout engine[r 1]	V8 engine[r 2]	Significant changes	Issues/Bugs

Major version	Release date	Layout engine[r 1]	V8 engine[r 2]	Significant changes	Issues/Bugs
				stability tweaks.[r 112]	
47.0.2526	2015-12-01 (iOS) 2015-12-01 (Linux, macOS, and Windows) 2015-12-02 (Android)	Blink 47 (except iOS)	4.7.80	■ Change in appearance on closing tabs with red x's ■ New PDF viewer design ■ Security fixes[r 113] Android version: ■ "More than a barge load of performance and stability fixes" [r 114] iOS version: ■ Added support for more keyboard shortcuts. Bluetooth keyboards can open, close or change tabs or conduct a voice search. ■ Support for 3D touch on iPhone 6s/+. Force touch the Chrome icon to quickly open a new tab, a new incognito* tab, or conduct a voice search.	
48.0.2564	2016-01-20 (Linux, macOS, and Windows) 2016-01-27 (iOS) 2016-01-27 (Android)	Blink 48 (except iOS)	4.8.271	■ "Tab discarding" was enabled by default in chrome://flags ■ Window change in right-clicking an embedded web link ■ The key icon in "Save your password" turns black ■ "Clear browsing history" has been improved ■ A large number of fixes and improvements[r 115] Android version: ■ Bug fixes and speedy performance improvements. iOS version: ■ This version uses WKWebView, the latest rendering engine from Apple. ■ The crash rate was reduced by 70% and JavaScript execution is now faster. ■ Redesigned icons on the New Tab page: easier access to more of your frequently-visited sites. ■ Spotlight integration: Drag down or right from the Home screen and search for your Chrome bookmarks.	
49.0.2623	2016-03-02 (Linux, macOS, and Windows) 2016-03-09 (iOS) 2016-03-09 (Android)	Blink 49 (except iOS)	4.9.385	■ Extension icons now appear near search tab. ■ Changes in bookmark bar appearances. ■ Change in Incognito mode window. ■ Change in scrollbar movement.	
Major version	Release date	Layout engine[r 1]	V8 engine[r 2]	Significant changes	Issues/Bugs

Major version	Release date	Layout engine[r 1]	V8 engine[r 2]	Significant changes	Issues/Bugs
				▪ Changed Downloads page appearance/design. ▪ A large number of fixes and improvements[r 116] ▪ Removed Windows 8 Mode (Metro mode) ▪ Removed support 32-bit Linux, Ubuntu Precise (12.04), and Debian 7 (wheezy). ▪ Last version supported on Windows XP and Vista, as well as Mac OS X 10.6, 10.7, and 10.8. Android version: ▪ "More than a barge full of performance and stability fixes."[r 117] iOS version: ▪ Bookmarks has a new look: Easily find your favorites! ▪ Bug and stability fixes.	
50.0.2661	2016-04-13 (Linux, macOS, and Windows) 2016-04-20 (iOS) 2016-04-26 (Android)	Blink 50 (except iOS)	5.0.71	▪ Windows XP, Vista, Mac OS X 10.6, 10.7, and 10.8 compatibility broken. ▪ Auto-fill form letters are now highlighted in bold. ▪ A number of fixes and improvements.[r 118] Android version: ▪ Bug fixes and speedy performance improvements. iOS version: ▪ Bug and stability fixes.	
51.0.2704	2016-05-25 (Linux, macOS, and Windows) 2016-06-01 (iOS) 2016-06-01 (Android)	Blink 51 (except iOS)	5.1.281	▪ A number of fixes and improvements.[r 119] Android version: ▪ Brought tab switching back into Chrome (Android L+)[r 120] ▪ Bug fixes and speedy performance improvements. iOS version: ▪ Bug and stability fixes.	
52.0.2743	2016-07-20 (Linux, macOS, and Windows) 2016-07-27 (iOS) 2016-07-27 (Android)	Blink 52 (except iOS)	5.2.361	▪ It is impossible to disable DirectWrite. ▪ Bar on the bottom now shows darker text when hovering your mouse over the link. ▪ "A number of fixes and improvements."[r 121]	
Major version	Release date	Layout engine[r 1]	V8 engine[r 2]	Significant changes	Issues/Bugs

Major version	Release date	Layout engine[r 1]	V8 engine[r 2]	Significant changes	Issues/Bugs
				Android version: • Bug fixes and speedy performance improvements[r 122] **iOS version:** • Accelerated Mobile Pages ("AMP") – news and articles from many of your favorite publishers will now load instantly. • Lightning bolt and "AMP" next to articles in the "Top Stories" section of search results indicate faster web page loading.	
53.0.2785	2016-08-31 (Linux, macOS, and Windows) 2016-09-07 (iOS) 2016-09-07 (Android)	Blink 53 (except iOS)	5.3.332	• New browser's inside look, including a new bookmark • "A number of fixes and improvements."[r 123] • 'Simplify page' option removed from 'Save as PDF'. • Shadow DOM v1[5] **Android version:** • Bug fixes and speedy performance improvements[r 124] • Muted autoplay for video[r 125] **iOS version:** • Chrome's History has a new look and it's now easier to review, find, and delete your browsing history. • Voice Search has been updated with a fresh look. Voice Search can now answer contextual questions such as "How tall is the Eiffel Tower?" followed by "When was it built?"	
54.0.2840	2016-10-12 (Linux, macOS, and Windows) 2016-10-19 (iOS) 2016-10-19 (Android)	Blink 54 (except iOS)	5.4.500	• "Other bookmarks" tab has changed appearance • The message "Right-click to play Adobe Flash Player" now appears while pages with Adobe Flash Player are loading. • "A number of fixes and improvements."[r 126] **Android version:** • Bug fixes and speedy performance improvements • View article suggestions for you on the new tab page • Play media in the background for sites that support it • Update saved passwords when you change or reset your password[r 127]	
Major version	**Release date**	**Layout engine**[r 1]	**V8 engine**[r 2]	**Significant changes**	**Issues/Bugs**

Case 4:20-cv-03664-YGR   Document 928-20   Filed 04/19/23   Page 353 of 405

Major version	Release date	Layout engine[r 1]	V8 engine[r 2]	Significant changes	Issues/Bugs
				iOS version: ■ No internet connection? Smile and tap the dinosaur ■ Fixed bookmark icons not displaying correctly ■ Fixed phone number detection issues in web pages ■ Stability improvements and bug fixes	
55.0.2883	2016-12-01 (Linux, macOS, and Windows) 2016-12-05 (iOS) 2016-12-06 (Android)	Blink 55 (except iOS)	5.5.372	■ The History page has changed and is no longer in "Settings" ■ Flash Player is now off by default for most sites ■ "A number of fixes and improvements."[r 128] ■ It is not possible to disable top level Material Design[r 129] **iOS version:** ■ You can swipe down or right from the iOS Home screen to search. Searching for "voice" or "incognito" enables you to start Chrome in Voice Search mode or in a new Incognito Tab, respectively. The appearance of items in Spotlight Search will only work for devices that support Spotlight Actions. ■ The folder named "All Bookmarks" has been removed from the Bookmarks view. You can access all your other devices' Bookmarks by clicking on the other folders. **Android version:** ■ Bug fixes and speedy performance improvements ■ Easily download music, videos, and even full web pages for viewing offline ■ View and share your downloads within Chrome ■ See misspelled words highlighted in text fields ■ Improvements to contextual search UI[r 130]	
56.0.2924	2017-01-25 (Linux, macOS, and Windows) 2017-02-01 (iOS) 2017-02-01 (Android)	Blink 56 (except iOS)	5.6.326	■ HTML5 enabled by default ■ Adobe Flash Player is automatically blocked for most sites that require the plugin ■ Labeling of unsecured HTTP sites ■ "A number of fixes and improvements."[r 131] **iOS version:**	
Major version	**Release date**	**Layout engine[r 1]**	**V8 engine[r 2]**	**Significant changes**	**Issues/Bugs**

Major version	Release date	Layout engine[r 1]	V8 engine[r 2]	Significant changes	Issues/Bugs
				- Scan a QR code or barcode by using 3D Touch on the app logo or searching for "QR" in Spotlight. - We've redesigned the tab switcher layout on iPad to make it easier to access your open sites. Android version: - Easily download music, videos, and even full web pages for viewing offline - View and share your downloads within Chrome - See misspelled words highlighted in text fields - Improvements to contextual search UI - Bug fixes and significant memory savings[r 132]	
57.0.2987	2017-03-09 (Linux, macOS, and Windows) 2017-03-14 (iOS) 2017-03-16 (Android)	Blink 57 (except iOS)	5.7.492	- CSS grid layout - Improved "Add to Home" screen - Media Session API - "A number of fixes and improvements."[r 133] - WebAssembly[r 134] - Background tab policy changes[6] - Removed the chrome://plugins page. iOS version: - Chrome can add pages to your Reading List. - Find in Page now works correctly in iOS 10.3. Android version: - Quickly use emails, addresses, and phone numbers in web pages by tapping on them - Easily access downloaded files and web pages from the new tab page - Long press article suggestions on the new tab page to download them - Bug fixes and performance improvements[r 135]	
58.0.3029	2017-04-19 (Linux, macOS, and Windows) 2017-04-20 (Android) 2017-04-25 (iOS)	Blink 58 (except iOS)	5.8.283	- "A number of fixes and improvements."[r 136] - IndexedDB 2.0 - Workers and SharedWorkers in data-URLs. Android version: - Useful actions like "Find in page" available in apps that open web	
Major version	Release date	Layout engine[r 1]	V8 engine[r 2]	Significant changes	Issues/Bugs

Major version	Release date	Layout engine[r 1]	V8 engine[r 2]	Significant changes	Issues/Bugs
				pages using Chrome ■ More frequently updated article suggestions on the New Tab page ■ Use recently visited search engines as your default search engine ■ See Physical Web suggestions, based on your surroundings, in the address bar ■ Bug fixes and performance improvements[r 137] iOS version: ■ Stability improvements and bug fixes.	
59.0.3071	2017-06-05 (Linux, macOS, and Windows) 2017-06-06 (iOS) 2017-06-06 (Android)	Blink 59 (except iOS)	5.9.211	■ "A number of fixes and improvements."[r 138] ■ Revamped Settings and "About Google Chrome" page with Material Design ■ Headless mode in Linux and macOS.[r 139] iOS version: ■ Fixed a user-reported issue that resulted in hangs and significant slowdowns when switching tabs. ■ Fixed a crash involving dialogs presented while switching tabs. ■ Stability improvements and bug fixes. Android version: ■ View and manage in-progress downloads on the Downloads page ■ View and clear your browsing data more easily on the redesigned History page ■ Long-press a link to open it in a new Chrome tab (from Chrome Custom Tabs) ■ Bug fixes and performance improvements[r 140]	
60.0.3112	2017-07-25 (Linux, macOS, and Windows) 2017-07-25 (iOS) 2017-07-31 (Android)	Blink 60 (except iOS)	6.0.286	■ MacBook Pro Touch Bar support. ■ "A number of fixes and improvements."[r 141] iOS version: ■ "Request Mobile Site" button can switch from a website's desktop version back to its mobile version Android version: ■ Load pages faster and use less memory with an updated JavaScript engine	
Major version	Release date	Layout engine[r 1]	V8 engine[r 2]	Significant changes	Issues/Bugs

Major version	Release date	Layout engine[r 1]	V8 engine[r 2]	Significant changes	Issues/Bugs
				- Bug fixes and performance improvements - Clear browsing data more easily[r 142]	
61.0.3163	2017-09-05 (Linux, macOS, and Windows) 2017-09-05 (iOS) 2017-09-05 (Android)	Blink 61 (except iOS)	6.1.534	- Native support for JavaScript modules "A number of fixes and improvements."[r 143] iOS version: - Added a new button for scanning QR codes above the virtual keyboard Android version: - Addition of Web Share API - Bug fixes and performance improvements - Translate pages with a more compact and intuitive toolbar - Pick images to post online with an improved image picker[r 144]	
62.0.3202	2017-10-17 (Linux, macOS, and Windows) 2017-10-18 (iOS) 2017-10-19 (Android)	Blink 62 (except iOS)	6.2.414	- The "Save Your Password" icon gets a new appearance "A number of fixes and improvements."[r 145] - Support for OpenType variable fonts - Network Information API updated to report users actual Internet speed, not just connection type, to websites - HTTP sites that request user data will now be flagged as "non-secure" (red) in the Chrome Omnibox[r 146] iOS version: - Two new Today widgets are added by tapping the Edit button at the bottom of the iOS Search screen - Ability to drag a URL from another app and drop it into Chrome's omnibox or the tab strip, or from Chrome's content area to another app on iOS 11 iPads - The Payment Request API has been introduced Android version: - Download files faster with accelerated downloads - View and copy passwords saved with Chrome if device lock is enabled - Quickly see your data savings in the Chrome menu when Data Saver is on[r 147]	
Major version	Release date	Layout engine[r 1]	V8 engine[r 2]	Significant changes	Issues/Bugs

Major version	Release date	Layout engine[r 1]	V8 engine[r 2]	Significant changes	Issues/Bugs
63.0.3239	2017-12-05 (iOS) 2017-12-05 (Android) 2017-12-06 (Linux, macOS, and Windows)	Blink 63 (except iOS)	6.3.292	- Various fixes from internal audits, fuzzing and other initiatives "A number of fixes and improvements."[r 148] - Browser allows you to import JavaScript modules dynamically - With async generator functions and the async iteration protocol, consumption or implementation of streaming data sources becomes streamlined - You can override the browser's default overflow scroll behavior with the CSS overscroll-behavior property[r 149] iOS version: - Swipe up on the New Tab Page to explore suggested content from the web - The ability to reorder bookmarks is back! Android version: - Chrome for Android will make permission requests modal dialogs "Stability and performance improvements."[r 150]	
64.0.3282	2018-01-23 (Android) 2018-01-24 (iOS) 2018-01-24 (Linux, macOS, and Windows)	Blink 64 (except iOS)	6.4.388	"A number of fixes and improvements."[r 151] - Audio playback rates of below 0.5 and above 4.0 supported due to new, high-quality algorithm for stretching audio: "WSOLA" (Waveform-Similarity-Overlap-Add)[7] - Android: "share" menu picks pages' canonical URL instead of full URL from address bar.[8] - Support for ResizeObservers, will notify you when an element's content rectangle has changed its size. - Modules can now access to host specific metadata with import.meta. - The pop-up blocker gets stronger. - window.alert() no longer changes tab focus. - Chrome now supports named captures in regular expressions. - The default preload value for <audio> and <video> elements is now metadata. - You can now use Request.prototype.cache to view the cache mode of a Request and determine whether a request is a reload request.	
Major version	Release date	Layout engine[r 1]	V8 engine[r 2]	Significant changes	Issues/Bugs

Major version	Release date	Layout engine[r 1]	V8 engine[r 2]	Significant changes	Issues/Bugs
				• Using the Focus Management API, you can now focus an element without scrolling to it with the preventScroll attribute.[r 152] • Extensions page generates packages in CRX3 format now.[r 153] Android version: • Prevents sites with abusive ad experiences from opening new windows or tabs without your permission. • "Stability and performance improvements."[r 154] iOS version: • You can now disable Article Suggestions without also disabling omnibox suggestions by going to Chrome Settings • If you previously turned off "Search and Site Suggestions" to disable Article Suggestions and would like to turn back on your Search Suggestions in the omnibox, you can do that from Chrome Settings > Privacy • Support for iPhone X • Now requires iOS 10 or later	
65.0.3325	2018-03-06 (Linux, macOS, and Windows) 2018-03-06 (iOS) 2018-03-06 (Android)	Blink 65 (except iOS)	6.5.254	• "A number of fixes and improvements."[r 155] • New extension UI • The CSS Paint API allows you to programmatically generate an image • The Server Timing API allows web servers to provide performance timing information via HTTP headers • The new CSS display: contents property can make boxes disappear • Fixed a bug that affected some timestamps • The syntax for specifying HSL and HSLA, and RGB and RGBA coordinates for the color property now match the CSS Color 4 spec • There's a new feature policy that allows you to control synchronous XHRs through an HTTP header or the iframe allow attribute[r 156] • Last version available for OS X 10.9. Android version: • Set language preferences for web content in Settings > Languages • Turn on the prompt for simplified view for all supported articles in Settings > Accessibility settings	
Major version	Release date	Layout engine[r 1]	V8 engine[r 2]	Significant changes	Issues/Bugs

Major version	Release date	Layout engine[r 1]	V8 engine[r 2]	Significant changes	Issues/Bugs
				■ Share and delete downloads more easily on the Downloads page[r 157] ■ Disable screen capture on incognito mode [9] iOS version: ■ Fixed a bug that affected some streaming audio players ■ Stability and performance improvements	
66.0.3359	2018-04-17 (Linux, macOS, and Windows) 2018-04-17 (iOS) 2018-04-17 (Android)	Blink 66 (except iOS)	6.6.346	■ "A number of fixes and improvements."[r 158] ■ CSS manipulation becomes easier with the new CSS Typed Model Object ■ Access to the clipboard is now asynchronous ■ There's a new rendering context for canvas elements ■ TextArea and Select now support the autocomplete attribute ■ Setting autocapitalize on a form element will apply to any child form fields, improving compatibility with Safari's implementation of autocapitalize ■ trimStart() and trimEnd() are now available as the standards-based way of trimming whitespace from strings[r 159] Android version: ■ Find your saved passwords more easily – just tap the new Search icon in Settings > Passwords[r 160] iOS version: ■ Export passwords saved in Chrome and use them in another app ■ Stability and performance improvements	
67.0.3396	2018-05-29 (Linux, macOS, and Windows) 2018-05-29 (iOS) 2018-05-31 (Android)	Blink 67 (except iOS)	6.7.288	■ "A number of fixes and improvements."[r 161] ■ Progressive Web Apps are coming to the desktop ■ The generic sensor API makes it way easier to get access to device sensors like the accelerometer, gyroscope and more ■ BigInt's make dealing with big integers way easier. ■ Credential Management API provides a framework for creating, retrieving and storing credentials ■ The Web Authentication API adds a	
Major version	Release date	Layout engine[r 1]	V8 engine[r 2]	Significant changes	Issues/Bugs

Major version	Release date	Layout engine[r 1]	V8 engine[r 2]	Significant changes	Issues/Bugs
				third credential type, PublicKeyCredential, which allows browsers to authenticate a user with a private/public key pair generated by an authenticator[r 162] Android version: ▪ "Stability and performance improvements."[r 163] iOS version: ▪ Improved handling of boarding passes, movie tickets, etc. in Wallet ▪ Updated app selection UI when you tap on an email link ▪ Improved support for external keyboards ▪ Improved issue reporting: now you can draw on screenshots you are sending with feedback reports to obscure private data ▪ A fix has been provided for autofill issue (June 13)	
68.0.3440	2018-07-24 (iOS) 2018-07-24 (Linux, macOS, and Windows) 2018-07-24 (Android)	Blink 68 (except iOS)	6.8.275	▪ "A number of fixes and improvements." ▪ HTTP sites marked as "not secure".[r 164] ▪ The Page Lifecycle API tells you when your tab has been suspended or restored. ▪ The Payment Handler API makes it possible for web-based payment apps to support the Payment Request experience. ▪ Content embedded in an iframe requires a user gesture to navigate the top-level browsing context to a different origin. ▪ Since Chrome 1, the CSS cursor values for grab and grabbing have been prefixed; standard, un-prefixed values now supported [r 165] Android version: ▪ Fix for an Autofill issue.[r 166] ▪ The Add to Home Screen behavior on Android is changing to give you more control. iOS version: ▪ Improved downloading from websites. Downloading now works while the app is in the background. You can also continue browsing in the same tab while your file downloads. ▪ Improvements to Forms Autofill.	
Major version	Release date	Layout engine[r 1]	V8 engine[r 2]	Significant changes	Issues/Bugs

Major version	Release date	Layout engine[r 1]	V8 engine[r 2]	Significant changes	Issues/Bugs
				• Improved handling of links to the App Store.	
69.0.3497	2018-09-04 (Linux, macOS, and Windows) 2018-09-04 (iOS) 2018-09-04 (Android)	Blink 69 (except iOS)	6.9.427	• "A number of fixes and improvements."[r 167] • New browser interface • CSS Scroll Snap allows you to create smooth, slick, scroll experiences. • Display Cutouts lets you use the full area of the screen, including any space behind the display cutout, sometimes called a notch. • The Web Locks API allows you to asynchronously acquire a lock, hold it while work is performed, then release it. • You can now create color transitions around the circumference of a circle, using conic gradients. • New toggleAttribute() method on elements toggles the existence of an attribute, similar to classList.toggle(). • JavaScript arrays are getting two new methods: flat() and flatMap(). • OffscreenCanvas moves work off the main thread in a worker, helping to eliminate performance bottlenecks.[r 168] Android version: • Secure and easy mobile payments via 3rd party payment apps • Password generation now works on more sites[r 169] iOS version: • New bottom toolbar: easier to reach frequently used functions, like Back, Search, tabs, and the menu • New tab grid: see bigger previews of your tabs, including tabs open on other devices • Features like Bookmarks and Reading Lists are now easily accessible on the New Tab Page • Press firmly on the app icon to see shortcuts (3D Touch) • Credit cards you enter on your device are now securely synced to Google Pay for use on other devices (if enabled)	
70.0.3538	2018-10-16 (Linux, macOS, and Windows) 2018-10-16 (iOS) 2018-10-17 (Android)	Blink 70 (except iOS)	7.0.276	• "A number of fixes and improvements."[r 170] • Desktop Progressive Web Apps on Windows • The credential management API adds support for Public Key	
Major version	Release date	Layout engine[r 1]	V8 engine[r 2]	Significant changes	Issues/Bugs

Major version	Release date	Layout engine[r 1]	V8 engine[r 2]	Significant changes	Issues/Bugs
				Credentials ■ Named workers ■ Web Bluetooth is now available in Windows 10 ■ Chrome can send intervention and deprecation messages to your servers using the Report-To HTTP Response header field or surface them in the ReportingObserver interface ■ Support for AV1 video decoder ("Main" profile 0)[r 171] ■ A number of important deprecations[r 172] Android version ■ "Stability and performance improvements"[r 173] ■ Cleaner, more modern design iOS version: ■ Bug fixes and design polish for the redesign ■ Updates to how Chrome launches other apps to improve reliability and security ■ Fixes to authentication issues caused by using out-of-date cookies	
71.0.3578	2018-12-04 (Linux, macOS, and Windows) 2018-12-04 (iOS) 2018-12-04 (Android)	Blink 71 (except iOS)	7.1.302	■ "A number of fixes and improvements."[r 174] ■ Displaying relative times is now part of the Intl API ■ Specifying which side of the text the underline should appear on for text that flows vertically ■ Requiring user activation before using the speech synthesis API ■ The default credentials mode for module script requests has changed from omit to same-origin ■ Shadow DOM v1 spec; calculation for specificity for the :host() and :host-context() pseudo classes as well as for the arguments for ::slotted()[r 175] ■ Removed SpeechSynthesis.speak() without user activation ■ Removed prefixed versions of APIs ■ Removed URL.createObjectURL from MediaStream ■ Removed document.origin ■ Deprecations and removals of APIs[r 176] Android version: ■ The Element.requestFullscreen()	
Major version	Release date	Layout engine[r 1]	V8 engine[r 2]	Significant changes	Issues/Bugs

Major version	Release date	Layout engine[r 1]	V8 engine[r 2]	Significant changes	Issues/Bugs
				method can now be customized ■ "Stability and performance improvements."[r 177] iOS version: ■ You can now long-press on an image and save to clipboard and paste in other apps ■ Autofill now works better on sites with iframes (embedded pages)	
72.0.3626	2019-01-29 (Linux, macOS, and Windows) 2019-01-29 (iOS) 2019-01-29 (Android)	Blink 72 (except iOS)	7.2.502	■ "A number of fixes and improvements."[r 178] ■ Creating public class fields in JavaScript is now much cleaner ■ New User Activation API ■ Localizing lists becomes way easier with the Intl.format() API ■ Chrome 72 changes the behavior of Cache.addAll() to better match the spec ■ Requests for favicons are now handled by the service worker, as long as the request URL is on the same origin as the service worker[r 179] ■ Pages may no longer use window.open() to open a new page during unload ■ Removal of HTTP-Based Public Key Pinning ■ Removal of rendering FTP resources ■ Deprecation of TLS 1.0 and TLS 1.1 ■ Deprecation of PaymentAddress.languageCode[r 180] Android version: ■ "Stability and performance improvements."[r 181] ■ No longer supports Android 4.1-4.3 (Jelly Bean)[10] iOS version: ■ Support for more search engines ■ Fixed crashes on some page translations and added translations on previously untranslated websites ■ A Siri Shortcut to start a new search is available	
73.0.3683	2019-03-12 (Linux, macOS, and Windows) 2019-03-12 (iOS) 2019-03-12 (Android)	Blink 73 (except iOS)	7.3.492	■ "A number of fixes and improvements."[r 182] ■ Creating portable content is easier with signed HTTP exchanges	
Major version	Release date	Layout engine[r 1]	V8 engine[r 2]	Significant changes	Issues/Bugs

Major version	Release date	Layout engine[r 1]	V8 engine[r 2]	Significant changes	Issues/Bugs
				- Dynamically changing styles becomes way easier with constructable style sheets - Support for Progressive Web Apps arrives on macOS, bringing support for PWAs to all desktop and mobile platforms - matchAll() is a new regular expression matching method on the string prototype, and returns an array containing the complete matches - The <link> element now supports imagesrcset and imagesizes properties to correspond to srcset and sizes attributes of HTMLImageElement - Blink's shadow blur radius implementation now matches Firefox and Safari - Dark mode is now supported on Mac, and Windows support is on the way[r 183] - Removal of EXPLAIN and REINDEX support in WebSQL - Removal of isomorphic decoding of URL fragment identifier - Deprecation of 'drive-by downloads' in sandboxed iframes[r 184] - Stoppage of support for external web extensions in CRX2 format, making CRX3 format required[r 185] Android version: - Offline Content on the Dino Page: easily browse suggested articles while offline - Lite pages: get optimized pages that save data and load faster[r 186] iOS version: - Tap on the icons above the keyboard and easily access your saved passwords, addresses and credit card information - Updated default search engines list - View JavaScript console messages	
74.0.3729	2019-04-23 (Linux, macOS, and Windows) 2019-04-24 (Android) 2019-04-29 (iOS)	Blink 74 (except iOS)	7.4.288	"A number of fixes and improvements."[r 187] - Creating private class fields in JavaScript is now much cleaner - You can detect when the user has requested a reduced motion experience - CSS transition events - Adds new feature policy APIs to check if features are enabled or not[r 188]	
Major version	Release date	Layout engine[r 1]	V8 engine[r 2]	Significant changes	Issues/Bugs

Major version	Release date	Layout engine[r 1]	V8 engine[r 2]	Significant changes	Issues/Bugs
				- Removal of PaymentAddress's languageCode property - No popups during page unload - Deprecation of drive-by downloads in sandboxed iframes[r 189] **Android version:** - Translate any web page instantly by selecting Translate from the menu[r 190] **iOS version:** - You can now paste pictures from your clipboard into the omnibox to search - A fix has been included for translation not being offered on some English pages.	
75.0.3770	2019-06-04 (Linux, macOS, and Windows) 2019-06-04 (iOS) 2019-06-04 (Android)	Blink 75 (except iOS)	7.5.288	"A number of fixes and improvements."[r 191] - A new way to reduce latency on canvas elements - Web apps can now share files to other installed apps using the system level share sheet - Numeric literals now allow underscores as separators to make them more readable[r 192] - Removal of overflow: -webkit-paged-x and overflow: -webkit-paged-y[r 193] **Android version:** - Generate strong and unique passwords with Chrome's built-in password manager - Quickly look up your passwords by tapping any password field and using the new keyboard option[r 194] **iOS version:** - Links that are clicked in Incognito mode will no longer open native applications - Custom search engine settings now show the search engine's icon	
76.0.3809	2019-07-30 (Linux, macOS, and Windows) 2019-07-30 (iOS) 2019-07-30 (Android)	Blink 76 (except iOS)	7.6.303	"A number of fixes and improvements."[r 195] - Support for prefers-color-scheme media query, bringing dark mode to websites - An install button in the omnibox to make installation of Progressive Web Apps on desktop easier - Addition of Promise.allSettled()	
Major version	Release date	Layout engine[r 1]	V8 engine[r 2]	Significant changes	Issues/Bugs

Major version	Release date	Layout engine[r 1]	V8 engine[r 2]	Significant changes	Issues/Bugs
				- Reading blobs is easier - Image support in the async clipboard API[r 196] - Removal of feature policy: lazyload - Removal of outputs from MediaStreamAudioDestinationNode - Removal of insecure usage of DeviceMotionEvent - Removal of insecure usage of DeviceOrientationEvent[r 197] Android version: "Stability and performance improvements."[r 198] - Preventing the mini-infobar from appearing on Progressive Web Apps on mobile - More frequent updates of WebAPKs iOS version: - Find In Page now works on iFrames, including AMP (Accelerated Mobile Pages) - A suggestion for a strong and unique password on a keyboard when signing up to a new site - Control of all Sync and Google services settings in one place - Some users will see a new design for the way Chrome offers to save passwords	
77.0.3865	2019-09-10 (Linux, macOS, and Windows) 2019-09-10 (iOS) 2019-09-10 (Android)	Blink 77 (except iOS)	7.7.299	- A number of fixes and improvements."[r 199] - Forms get some new capabilities - The formdata event - Form-associated custom elements - Native lazy loading - Chrome DevSummit 2019 is happening November 11–12, 2019 - Introduction of Content Picker API - New measurement units in the intl.NumberFormat API[r 200] - Removal of card issuer networks as payment method names - Deprecation of Web MIDI use on insecure origins - Deprecation of WebVR 1.1 API[r 201] Android version: "Stability and performance improvements."[r 202] - A better way to track the performance of your site with Largest	
Major version	Release date	Layout engine[r 1]	V8 engine[r 2]	Significant changes	Issues/Bugs

Major version	Release date	Layout engine[r 1]	V8 engine[r 2]	Significant changes	Issues/Bugs
				Contentful Paint **iOS version:** - A new language settings page - You can clear your browsing data from a specific range of time - Omnibox suggestions are easier to read with added thumbnails and icons - Easily close tabs that are maliciously showing JavaScript dialogues	
78.0.3904	2019-10-22 (iOS) 2019-10-22 (Android) 2019-10-22 (Linux, macOS, and Windows)	Blink 78 (except iOS)	7.8.279	"A number of fixes and improvements."[r 203] - CSS Properties and Values API - Fresher service workers - New origin trials - Native File System - SMS Receiver[r 204] - Removal of XSS Auditor[r 205] **Android version:** "Stability and performance improvements."[r 206] - Dark theme for Chrome menus, settings, and surfaces **iOS version:** - The ability to switch Chrome to dark mode if your device has been upgraded to iOS 13 - Bookmarks, History, Recent Tabs, and Reading List are now presented as cards on iOS 13 - The ability to add a new credit card directly in Chrome from the settings page - A fix for a navigation-related crash	
79.0.3945	2019-12-10 (iOS) 2019-12-10 (Linux, macOS, and Windows) 2019-12-10 (Android)	Blink 79 (except iOS)	7.9.317	"A number of fixes and improvements."[r 207] - The ability to create immersive experiences with the WebXR Device API - The Wake Lock API is available as an origin trial - The rendersubtree attribute is available as an origin trial - Videos from the Chrome DevSummit are now online[r 208] - Changes -webkit-appearance keywords to work only with specific element types[r 209] **Android version:**	
Major version	Release date	Layout engine[r 1]	V8 engine[r 2]	Significant changes	Issues/Bugs

Major version	Release date	Layout engine[r 1]	V8 engine[r 2]	Significant changes	Issues/Bugs
				"Stability and performance improvements." - Password safety - Support for virtual reality - The ability to reorder bookmarks[r 210] - Installed Progressive Web Apps on Android now support maskable icons iOS version: - Chrome will check if username and password are leaked if signed in to Chrome and then in to a website - Starting a search in the address bar will initiate top suggestions even if network connection is slow	
80.0.3987	2020-02-04 (Linux, macOS, and Windows) 2020-02-04 (Android) 2020-02-05 (iOS)	Blink 80 (except iOS)	8.0.426	"A number of fixes and improvements."[r 211] - Modules in workers - Optional chaining in JavaScript - New origin trials - Origin trial graduations - Using #:~:text=something will have Chrome scroll to and highlight the first instance of that text fragment - Setting display: minimal-ui on a Desktop PWA adds a back and reload button to the title bar of the installed PWA - Support for using SVG images as favicons[r 212] - Disallowed Synchronous XMLHTTPRequest() in Page Dismissal - Deprecation of FTP support - Removal of allowing popups during page reload - Non-origin-clean ImageBitmap serialization and transferring removed - Protocol handling now requires a secure context - Web Components v0 removed - Removal of -webkit-appearance:button for arbitrary elements[r 213] Android version: "Stability and performance improvements." - Quieter notifications - SameSite cookies are enabled by default - Insecure audio and video on secure pages are automatically upgraded to secure connections[r 214]	
Major version	Release date	Layout engine[r 1]	V8 engine[r 2]	Significant changes	Issues/Bugs

Major version	Release date	Layout engine[r 1]	V8 engine[r 2]	Significant changes	Issues/Bugs
				iOS version: ■ Starting a search in the address bar brings up top suggestions served locally even in Incognito Mode	
81.0.4044	2020-04-07 (Linux, macOS, and Windows) 2020-04-07 (Android) 2020-04-07 (iOS)	Blink 81 (except iOS)	8.1.307	■ "A number of fixes and improvements."[r 215] ■ Updated Chrome release schedule ■ WebXR hit testing ■ App icon badging ■ New origin trial of Web NFC and other origin trials ■ The media session API now supports tracking position state ■ INTL API now provides a DisplayNames method[r 216] ■ Deprecation and removal of "basic-card" support Payment Handler ■ Removal of supportedType field from BasicCardRequest ■ Removal of <discard> element ■ TLS 1.3 downgrade hardening bypass (Removal of TLS 1.0 and 1.1 is delayed to Chrome 84 due to the COVID-19 pandemic.)[r 217] Android version: ■ "Stability and performance improvements." ■ 27 languages were added, including Burmese, Armenian, Urdu, Central Khmer, and Punjabi ■ Notification of whether a password is typed and saved on an unsafe site[r 218] iOS version: ■ Updated Terms of Service ■ Finding downloads in the downloads folder in Chrome's menu or in the device's Files app ■ Search suggestions will also include suggestions from the middle of words ■ Fixes for crashes related to bookmarks and security	
83.0.4103	2020-05-19 (Linux, macOS, and Windows) 2020-05-19 (Android) 2020-05-21 (iOS)	Blink 83 (except iOS)	8.3.110	■ Version 82 was skipped due to the COVID-19 pandemic. ■ "A number of fixes and improvements."[r 219] ■ Trusted types help prevent cross site scripting vulnerabilities ■ Form elements get an important make-over ■ A new way to detect memory leaks	
Major version	Release date	Layout engine[r 1]	V8 engine[r 2]	Significant changes	Issues/Bugs

Major version	Release date	Layout engine[r 1]	V8 engine[r 2]	Significant changes	Issues/Bugs
				■ The native file system API starts a new origin trial with added functionality ■ New cross-origin policies ■ The Web Vitals program provides unified guidance for quality signals that are essential to delivering a great user experience on the web ■ Chrome now supports the Barcode Detection API, which provides the ability to detect and decode barcodes ■ The new CSS @supports function provides feature detection for CSS selectors ■ New ARIA annotations support screen reader accessibility for comments, suggestions, and text highlights with semantic meanings (similar to <mark>) ■ The prefers-color-scheme media query lets authors support their own dark theme so they have full control over experiences they build ■ JavaScript now supports modules in shared workers[r 220] ■ Disallowing of downloads in Sandboxed iframes[r 221] Android version: ■ No longer supports Android 4.4 (KitKat)[r 222] ■ "Stability and performance improvements."[r 223] iOS version: ■ Allows users to see their last 5 search queries by tapping the address bar in a new tab when signed in with a Google account ■ Prompts and messages from Chrome have a refreshed look ■ iPhone users can change webpage text to a comfortable size by opening Chrome's menu and tapping "Zoom Text..." or by going to their Accessibility settings ■ Updated Terms of Service.	
84.0.4147	2020-07-14 (Linux, macOS, and Windows) 2020-07-14 (iOS) 2020-07-14 (Android)	Blink 84 (except iOS)	8.4.371	■ "A number of fixes and improvements."[r 224] ■ App Icon Shortcuts ■ The Web Animations API adds support for a slew of previously unsupported features ■ Wake lock can prevent the screen from dimming or locking ■ The Content Indexing API helps surface content that is available	Windows: ■ Lightbox (JavaScript) (window inside window) no longer functions properly in Chromium based
Major version	Release date	Layout engine[r 1]	V8 engine[r 2]	Significant changes	Issues/Bugs

Major version	Release date	Layout engine[r 1]	V8 engine[r 2]	Significant changes	Issues/Bugs
				offline ■ New origin trials for idle detection and Web Assembly SIMD ■ Same Site Cookie policy changes are starting to roll out again ■ Sites with abusive permission requests, or abusive notifications, will automatically be enrolled in our quieter notifications UI ■ New origin trial for QuicTransport[r 225] ■ @import rules in CSSStyleSheet.replace() removed ■ Removal of TLS 1.0 and TLS 1.1[r 226] Android version: ■ "Stability and performance improvements."[r 227] iOS version: ■ New Safe Browsing features ■ Better mouse and trackpad support ■ You can now share a web page by creating and sharing a QR code ■ You can find your downloads in the downloads folder in Chrome's menu, or in your device's Files app ■ Addition of nicknames to your payment cards saved in Chrome[r 228]	browsers.[11]
85.0.4183	2020-08-25 (Linux, macOS, and Windows) 2020-08-25 (iOS) 2020-08-25 (Android)	Blink 85 (except iOS)	8.5.210	■ "A number of fixes and improvements."[r 229] ■ AppCache Removal Begins ■ Rejection of insecure SameSite=None cookies ■ -webkit-box quirks from -webkit-line-clamp[r 230] iOS version: ■ Ability to use passwords saved to Chrome in other apps on the device ■ Site information has a new look ■ Users can drag links between the apps when another app is open next to Chrome in split view[r 231] ■ Fixes for clipboard crash and stability improvements Android version: ■ "Stability and performance improvements."[r 232]	
86.0.4240	2020-09-30 (iOS) 2020-10-06 (Android) 2020-10-06	Blink 86 (except iOS)	8.6.395	■ "A number of fixes and improvements."[r 233]	
Major version	Release date	Layout engine[r 1]	V8 engine[r 2]	Significant changes	Issues/Bugs

Major version	Release date	Layout engine[r 1]	V8 engine[r 2]	Significant changes	Issues/Bugs
	(Linux, macOS, and Windows)			• The File System Access API is now available • New origin trials for Web HID and the Multi-screen Window Placement API • The new CSS selector, :focus-visible, lets the user opt-in to the same heuristic the browser uses when it's deciding whether to display the default focus indicator • The user can customize the color, size, or type of number or bullet for lists with the CSS ::marker Pseudo-Element[r 234] • Removal of WebComponents v0 • Deprecation of FTP support[r 235] Android version: • "Stability and performance improvements."[r 236] iOS version: • Ability to make Chrome the default browser • Ability to check if saved passwords have been compromised and, if so, how to fix them • More sharing, opening, and other options when user taps and holds Bookmarks, history, recent tabs, and read later • Improvements to the personalized stories on New tab page • Chrome will offer some additional protection by checking known phishing websites with Google in real time if "Make searches and browsing better" is turned on.	
87.0.4280	2020-11-17 (Linux, macOS, and Windows) 2020-11-17 (Android) 2020-11-18 (iOS)	Blink 87 (except iOS)	8.7.220	• Automatic live captions for English video and audio.[12][13] • "A number of fixes and improvements."[r 237] • Users can now control pan, tilt, and zoom on webcams that support it • Range requests and service workers don't require as many workarounds • The font access API starts its origin trial • Flash Player end of support notifications now displaying at every launch unless Flash is disabled. • Transferable Streams - ReadableStream, WritableStream, and TransformStream objects can now be passed as arguments to postMessage() • Implemented most granular flow-relative features of the CSS Logical	
Major version	Release date	Layout engine[r 1]	V8 engine[r 2]	Significant changes	Issues/Bugs

Major version	Release date	Layout engine[r 1]	V8 engine[r 2]	Significant changes	Issues/Bugs
				Properties and Values spec, including shorthands and offsets to make these logical properties and values a bit easier to write ■ New @font-face descriptors have been added to ascent-override, descent-override, and line-gap-override to override metrics of the font ■ Several new text-decoration and underline properties ■ A number of changes related to cross-origin isolation[r 238] ■ Removal of comma separator in iframe allow attribute ■ Removal of -webkit-font-size-delta ■ Deprecation of FTP support[r 239] ■ Altered macOS icon to match the design style of MacOS Big Sur Android version: ■ "Stability and performance improvements."[r 240] iOS version ■ Users can now have multiple windows of Chrome at the same time on their iPad ■ New feature in Settings: Safety Check ■ Auto-fill is now more secure[r 241]	
88.0.4324	2021-01-19 (Linux, macOS, and Windows) 2021-01-19 (Android)	Blink 88 (except iOS)	8.8.278	■ "A number of fixes and improvements."[r 242] ■ Users can now upload extensions using manifest v3 to the Chrome Web Store ■ CSS aspect-ratio property ■ Heavy throttling of chained JavaScript timers ■ Play billing in Trusted Web Activity ■ To conform to a change in the HTML standard, anchor tags with target="_blank" will now imply rel="no-opener" by default ■ Pointer Lock API allows users to disable mouse acceleration ■ addEventListener now takes an Abort Signal as an option[r 243] ■ No popups during page unload (enterprises) ■ Web Components v0 removed ■ Dropped support for OS X Yosemite ■ FTP support disabled[r 244] Android version:	
Major version	Release date	Layout engine[r 1]	V8 engine[r 2]	Significant changes	Issues/Bugs

Major version	Release date	Layout engine[r 1]	V8 engine[r 2]	Significant changes	Issues/Bugs
				■ "Stability and performance improvements."[r 245] iOS version: ■ Chrome 88 has been skipped over due to many Google products not updating in iOS since November 2020.[r 246][r 247]	
89.0.4389	2021-03-02 (Linux, macOS, and Windows) 2021-03-02 (Android)	Blink 89 (except iOS)	8.9.255	■ "A number of fixes and improvements."[r 248] ■ WebHID, WebNFC, and Web Serial are now available ■ Closed a loophole a few developers used to skirt the PWA installability checks ■ The arrival of Web Share and Web Share Target ■ Chrome now allows top level await within JavaScript modules ■ Updated icon shown in the omnibox for installable PWAs ■ Allowed users to sign up for the Digital Goods API origin trial if they have used a Trusted Web Activity to make their PWA available in the Play Store for Chrome OS[r 249] ■ Removal of legacy prefixed events (webkitprerenderstart, webkitprerenderstop, webkitprerenderload, and webkitprerenderdomcontentloaded) dispatched on <link rel=prerender> ■ Stopped cloning sessionStorage for windows opened with noopener number[r 250] ■ Dropped support for older x86 processors that don't support SSE3[r 251] Android version: ■ "Stability and performance improvements."[r 252] iOS version: ■ Chrome 89 has been skipped over due to many Google products not updating in iOS since November 2020.[r 246][r 247]	
90.0.4430	2021-04-13 (Android) 2021-04-14 (Linux, macOS, and Windows) 2021-05-10 (iOS)	Blink 90 (except iOS)	9.0.257	■ "A number of fixes and improvements."[r 253] ■ A new value for the CSS overflow property ■ The Feature Policy API has been renamed to Permissions Policy ■ A new way to implement and use	
Major version	**Release date**	**Layout engine[r 1]**	**V8 engine[r 2]**	**Significant changes**	**Issues/Bugs**

Major version	Release date	Layout engine[r 1]	V8 engine[r 2]	Significant changes	Issues/Bugs
				Shadow DOM directly in HTML - Chrome's address bar will use https:// by default - AV1 encoder in desktop that is specifically optimized for video conferencing with WebRTC integration[r 254] - Removal of Content Security Policy directive 'plugin-types' - Removal of WebRTC RTP data channels - Return of empty for navigator.plugins and navigator.mimeTypes[r 255] Android version - "Stability and performance improvements."[r 256] iOS version - Search and Dino widgets available on iOS 14 - Users can edit saved usernames and passwords in Chrome Settings - Stability and performance improvements.[r 257]	
91.0.4472	2021-05-25 (Android) 2021-05-25 (Linux, macOS, and Windows) 2021-06-03 (iOS)	Blink 91 (except iOS)	9.1.269	- "A number of fixes and improvements."[r 258] - Web apps that interact with files can now suggest file names and directories when using the File System Access API - The user can read files from the clipboard - If the website has more than one domain, and they share the same account management backend, the user can tell Chrome they're the same, allowing the password manager to suggest the right credentials - Web Transport-previously called Quic Transport has undergone a number of changes and is starting a new origin trial - Web Assembly SIMD has finished its origin trial and is available to all users - The <link> element's media attribute will be honored for link rel="icon", meaning the user can define different icons based on media queries[r 259] Android version: - "Stability and performance improvements."[r 260] - The refreshed form elements have finally landed on Android, improving the user experience	Tab Grid View can no longer be disabled[r 262]
Major version	Release date	Layout engine[r 1]	V8 engine[r 2]	Significant changes	Issues/Bugs

Major version	Release date	Layout engine[r 1]	V8 engine[r 2]	Significant changes	Issues/Bugs
				iOS version: • Stability and performance improvements.[r 261]	
92.0.4515	2021-07-20 (iOS) 2021-07-20 (Linux, macOS, and Windows) 2021-07-20 (Android)	Blink 92 (except iOS)	9.2.230	• "A number of fixes and improvements."[r 263] • Removal of payment handlers for standardized payment method identifiers[r 264] Android version: • "Stability and performance improvements."[r 265] iOS version: • Users can take a screenshot of the whole webpage, then look for the "Full Page" option at the top of the screenshot editor • Users can add more security to their Incognito tabs with Touch ID, Face ID, or a Passcode • New Discover design on the New Tab Page makes exploring interests easier • The ability to ask for confirmation if users want to close all tabs from the Tab Switcher • Users can share, bookmark, and add individual tabs to their reading list from the Tab Switcher • Stability and performance improvements.[r 266] • Final version for iOS 12	
93.0.4577	2021-08-31 (iOS) 2021-08-31 (Linux, macOS, and Windows) 2021-08-31 (Android)	Blink 93 (except iOS)	9.3.345	• "A number of fixes and improvements."[r 267] • Users can now load CSS style sheets with import statements, just like JavaScript modules • Installed PWAs can register as URL handlers, making it possible for users to jump straight into their PWA • The Multi-Screen Window Placement API has been updated based on feedback and starts a second origin trial • Shortened release cycle • Flexbox and flexbox items have added support for the alignment keywords: start, end, self-start, self-end, left, and right • The async clipboard API now supports SVG files • The media attribute will be honored when setting meta theme-color[r 268]	
Major version	Release date	Layout engine[r 1]	V8 engine[r 2]	Significant changes	Issues/Bugs

Major version	Release date	Layout engine[r 1]	V8 engine[r 2]	Significant changes	Issues/Bugs
				- Blocked ports 989 and 990 - Removal of 3DES in TLS - Deprecation of WebAssembly cross-origin module sharing[r 269] Android version: - "Stability and performance improvements."[r 270] iOS version: - Updated context menu when users tap and hold a link or image in a web site - Users already signed in to a Google Account can now sign in more easily to Chrome and other Google services on the web - Signed-in users can now both use and save payment methods from their Google Account, without sync - Stability and performance improvements[r 271] - Final version for iOS 13	
94.0.4606	2021-09-21 (iOS) 2021-09-21 (Linux, macOS, and Windows) 2021-09-21 (Android)	Blink 94 (except iOS)	9.4.146	- "A number of fixes and improvements."[r 272] - The default color space for \<canvas\> elements is now formally defined in the spec as *SRGB*, and users can change it to *Display P3* - WebCodecs is a new, low level way to access built in audio and video codecs, important for streaming games, video editors, and such - WebGPU starts its origin trial - The prioritized scheduler.postTask() method allows users to schedule tasks, and dynamically change their priorities, or cancel them all together - The scrollbar-gutter property provides control over the presence of scrollbar gutters, allowing users to prevent layout changes as content expands - Virtual keyboard API gives users more control over how and when the virtual, on-screen keyboard is shown[r 273] - Deprecation and removal of WebSQL in third-party contexts - Restriction of private network requests for subresources to secure contexts[r 274] Android version: - "Stability and performance improvements."[r 275]	
Major version	Release date	Layout engine[r 1]	V8 engine[r 2]	Significant changes	Issues/Bugs

Major version	Release date	Layout engine[r 1]	V8 engine[r 2]	Significant changes	Issues/Bugs
				iOS version: - Users can now act on multiple tabs at once - Stability and performance improvements[r 276] - Now requires iOS 14	
95.0.4638	2021-10-19 (iOS) 2021-10-19 (Linux, macOS, and Windows) 2021-10-19 (Android)	Blink 95 (except iOS)	9.5.172	- "A number of fixes and improvements."[r 277] - Routing gets easier with URLPattern baked into the browser - The Eye Dropper API provides a built in tool for selecting colors - There's a new origin trial that allows users to opt into receiving the reduced UA string now - The PWA Summit videos are all online - For users following the Storage Foundation API work, there's a new origin trial for Access Handles - WebAssembly now provides exception handling support, which allows code to break control flow when an exception is thrown[r 278] - Removal of FTP support - Support for URLs with non-IPv4 hostnames ending in numbers - Deprecation of WebAssembly cross-origin module sharing - Deprecation of U2F API (Cryptotoken)[r 279] Android version: - "Stability and performance improvements."[r 280] iOS version: - Users can now download .mobileconfig files - Stability and performance improvements[r 281]	
96.0.4664	2021-11-09 (iOS) 2021-11-15 (Linux, macOS, and Windows) 2021-11-15 (Android)	Blink 96 (except iOS)	9.6.180	- "A number of fixes and improvements."[r 282] - Manifest id for PWAs - URL protocol handlers for PWAs - Priority hints (origin trial) - Emulation of Chrome 100 in the UA string - The Back, forward cache – or bfcache – is now available in stable, and brings Chrome in line with both Firefox and Safari[r 283] - Deprecation of "basic-card" method of PaymentRequest API[r 284]	
Major version	Release date	Layout engine[r 1]	V8 engine[r 2]	Significant changes	Issues/Bugs

Major version	Release date	Layout engine[r 1]	V8 engine[r 2]	Significant changes	Issues/Bugs
				Android version: - No longer supports Android 5 (Lollipop)[r 285] - "Stability and performance improvements."[r 286] **iOS version:** - Stability and performance improvements[r 287]	
97.0.4692	2022-01-04 (iOS) 2022-01-04 (Linux, macOS, and Windows) 2022-01-04 (Android)	Blink 97 (except iOS)	9.7.106	- "A number of fixes and improvements."[r 288] - WebTransport is a new option for sending real time messages between the client and server - Users can use feature detection to see what types of scripts a browser supports - Searching arrays from the end becomes a little easier - New lines in form entries are now normalized in the same way as Gecko and WebKit, improving interoperability between browsers - Client hint names are standardized by prefixing them with sec-ch - Closed <details> elements are now searchable and can be linked to[r 289] - Removal of SDES key exchange for WebRTC - Removal of WebSQL in third-party contexts - Removal of SDP Plan B[r 290] **Android version:** - "Stability and performance improvements."[r 291] **iOS version:** - Stability and performance improvements[r 292]	
98.0.4758	2022-02-01 (iOS) 2022-02-01 (Linux, macOS, and Windows) 2022-02-01 (Android)	Blink 98 (except iOS)	9.8.177	- "A number of fixes and improvements."[r 293] - COLRv1 font support - CORS preflight requests are now sent ahead of private network requests for subresources, asking for explicit permission from the target server - New origin trial for Region Capture, an API for cropping a self-capture video track[r 294] - Removal of SDES key exchange for WebRTC[r 295]	
Major version	**Release date**	**Layout engine**[r 1]	**V8 engine**[r 2]	**Significant changes**	**Issues/Bugs**

Major version	Release date	Layout engine[r 1]	V8 engine[r 2]	Significant changes	Issues/Bugs
				Android version: ▪ "Stability and performance improvements."[r 296] ▪ Opting out of auto-dark themes on Android **iOS version:** ▪ Users can now add or edit site passwords anytime in Chrome Settings > Passwords ▪ Stability and performance improvements[r 297]	
99.0.4844	2022-03-01 (iOS) 2022-03-01 (Linux, macOS, and Windows) 2022-03-01 (Android)	Blink 99 (except iOS)	9.9.115	▪ "A number of fixes and improvements."[r 298] ▪ CSS cascade layers gives users more control over their CSS, and helps to prevent style-specificity conflicts ▪ showPicker() for input elements ▪ The Canvas2D API has been updated, adding new functionality ▪ New origin trial to allow PWAs to provide alternate colors in the web app manifest for dark mode ▪ Handwriting recognition API[r 299] ▪ Removal of Battery Status API on insecure origins ▪ Removal of font-family -webkit-standard ▪ Removal of GamepadList ▪ Updated WebCodecs to match the specification[r 300] **Android version:** ▪ "Stability and performance improvements."[r 301] **iOS version:** ▪ Users can easily see their most visited sites, bookmarks, Discover content and more when they open a new tab ▪ Users can track price drops on products ▪ Stability and performance improvements[r 302]	
100.0.4896	2022-03-29 (iOS) 2022-03-29 (Linux, macOS, and Windows) 2022-03-29 (Android)	Blink 100 (except iOS)	10.0.139	▪ "A number of fixes and improvements."[r 303] ▪ New Chrome logo ▪ Reduced User-Agent string ▪ Multi-screen window placement API ▪ New forget() method for HID Devices that allow users to revoke a	
Major version	**Release date**	**Layout engine[r 1]**	**V8 engine[r 2]**	**Significant changes**	**Issues/Bugs**

Major version	Release date	Layout engine[r 1]	V8 engine[r 2]	Significant changes	Issues/Bugs
				permission to an HID Device that was granted by others ■ makeReadOnly() method allows users to make NFC tags permanently read-only.[r 304] ■ Last version for unreduced user-agent string[r 305] Android version: ■ "Stability and performance improvements."[r 306] iOS version: ■ Stability and performance improvements[r 307]	
101.0.4951	2022-04-26 (iOS) 2022-04-26 (Linux, macOS, and Windows) 2022-04-26 (Android)	Blink 101 (except iOS)	10.1.124	■ "A number of fixes and improvements."[r 308] ■ Reducing user agent string information ■ Removal of WebSQL in third-party contexts[r 309] Android version: ■ "Stability and performance improvements."[r 310] iOS version: ■ In the Discover feed, users can now see a live preview of a story by long pressing on it ■ Stability and performance improvements[r 311]	
102.0.5005	2022-04-20 (iOS) 2022-04-28 (Linux, macOS, and Windows) 2022-04-28 (Android)	Blink 102 (except iOS)	10.2	Current Beta channel	
103.0	2022-04-19 (iOS) 2022-04-28 (Linux, macOS, and Windows) 2022-04-28 (Android)	Blink 103 (except iOS)	10.3	Current Dev channel	
103.0	2022-04-16 (macOS and Windows) 2022-04-16 (Android)	Blink 103	10.3	Current Canary channel	
Major version	Release date	Layout engine[r 1]	V8 engine[r 2]	Significant changes	Issues/Bugs

See also

- Safari version history
- Firefox version history

Notes

- Release date is the date of first release. All channels have subsequent updates which are not shown. For release update history see Google Chrome Releases (https://chromereleases.googleblog.com/).

- Old development and beta builds are not shown after they become stable releases.
- The first stable release in macOS and Linux was Google Chrome 5.0.375. The first stable release on Android was Chrome 18.0.1025123 (Chrome for Android).[r 312][r 313][r 314]
- Chrome 21 was the last supported version on Mac OS X 10.5.
- As of Chrome 26, Linux installations of the browser may be updated only on systems that support GCC v4.6 and GTK v2.24 or later. Thus systems such as Ubuntu Lucid 10.04 LTS, Debian 6's 2.20, and RHEL 6's 2.18 are now among those marked as deprecated.[r 315]
- Chrome 34 was the last supported version to run on older processors that lacked SSE2.
- As of Chrome 59, Linux Chrome defaults to GTK+3. Older versions of Linux, e.g. RHEL 6 or CentOS 6, with only GTK+2 support, are not able to run this version of Chrome. Red Hat's GTK+2 build of Firefox ESR is probably the last remaining regularly updated browser on RHEL 6/CentOS 6.[14]
- Chrome 49 released on 2016-03-02 was the last version supported on Windows XP, Windows Vista, Mac OS X 10.6, 10.7, and 10.8.
- Standalone builds can be found on Google's Chromium Browser Continuous build server (http://commondatastorage.googleapis.com/chromium-browser-continuous/index.html).
- Chrome 67 was the last version supported on OS X 10.9, however, Google's download page offers version 65.
- Version 82 was skipped due to the COVID-19 pandemic.
- Chrome 87 was the last version supported on OS X 10.10.
- Chrome 95 was the last version supported on Android Lollipop.

References

1. "OmahaProxy CSV Viewer" (https://omahaproxy.appspot.com/).
2. "Refs - v8/v8.git - Git at Google" (https://chromium.googlesource.com/v8/v8.git/+refs). Retrieved May 16, 2015.
3. "A fresh take on the browser" (http://googleblog.blogspot.com/2008/09/fresh-take-on-browser.html). September 1, 2008. Retrieved July 11, 2012.
4. "Google Chrome Releases: Stable Update: Google Chrome 2.0.172.28" (http://googlechromereleases.blogspot.com/2009/05/stable-update-google-chrome-2017228.html).
5. "Stable Channel Update" (https://chromereleases.googleblog.com/2009/09/stable-channel-update.html). *Chrome Releases*. September 15, 2009. Retrieved July 14, 2021.
6. Laforge, Anthony. "Stable Channel Update" (http://googlechromereleases.blogspot.com/2010/01/stable-channel-update_25.html). Retrieved May 25, 2010.
7. "Google Chrome Releases: Stable Channel Update March 17, 2010" (http://googlechromereleases.blogspot.com/2010/03/stable-channel-update.html). googlechromereleases.blogspot.com. March 17, 2010. Retrieved April 8, 2012.
8. Rakowski, Brian (May 25, 2010). "Evolving from beta to stable with a faster version of Chrome" (http://googleblog.blogspot.com/2010/05/evolving-from-beta-to-stable-with.html). Retrieved May 25, 2010.
9. "Adobe Flash Player support now enabled in Google Chrome's stable channel" (http://chrome.blogspot.com/2010/06/adobe-flash-player-support-now-enabled.html). June 30, 2010. Retrieved August 8, 2010.
10. Rakowski, Brian (May 25, 2010). "A new Chrome stable release: Welcome, Mac and Linux!" (http://chrome.blogspot.com/2010/05/new-chrome-stable-release-welcome-mac.html). Retrieved August 28, 2014.
11. "Bringing improved PDF support to Google Chrome" (https://blog.chromium.org/2010/06/bringing-improved-pdf-support-to-google.html). Chromium Blog. June 17, 2010. Retrieved October 24, 2010.
12. "Bringing another Chrome release to you, right on time" (http://chrome.blogspot.com/2010/10/bringing-another-chrome-release-to-you.html). Retrieved October 24, 2010.
13. "Stable, Beta Channel Updates" (http://googlechromereleases.blogspot.com/2010/12/stable-beta-channel-updates.html). Retrieved December 3, 2010.
14. "Safer plug-ins, faster search, and richer graphics" (http://chrome.blogspot.com/2010/12/safer-plug-ins-faster-search-and-richer.html). Retrieved December 17, 2010.
15. "WebP Home" (https://developers.google.com/speed/webp/). Google Inc. Retrieved February 3, 2011.
16. "Dev Channel Update" (http://googlechromereleases.blogspot.com/2011/01/chrome-dev-release.html). Retrieved January 21, 2011.
17. "Issue 48607: Sandbox GPU process" (https://code.google.com/p/chromium/issues/detail?id=48607). Retrieved March 21, 2012.
18. "A New Crankshaft for V8" (https://blog.chromium.org/2010/12/new-crankshaft-for-v8.html). Retrieved December 17, 2010.
19. "Chrome Releases: Chrome Stable Release" (http://googlechromereleases.blogspot.com/2011/03/chrome-stable-release.html). googlechromereleases.blogspot.com. March 8, 2011. Retrieved April 8, 2012.
20. "Chrome Beta Release" (http://googlechromereleases.blogspot.com/2011/03/chrome-beta-release.html). March 22, 2011. Retrieved March 23, 2011.
21. Rura, Steve (March 2011). "A fresh take on an icon" (http://chrome.blogspot.com/2011/03/fresh-take-on-icon.html). Retrieved March 22, 2011.
22. "Chrome Stable Release" (http://googlechromereleases.blogspot.com/2011/06/chrome-stable-release.html). June 7, 2011. Retrieved June 7, 2011.

23. "Google Operating System: Chrome shifts into a new gear" (http://googlesystem.blogspot.com/2011/06/chrome-shifts-into-new-gear.html). *Google Operating System*. June 7, 2011. Retrieved February 4, 2012.

24. Bentzel, Chris (June 16, 2011). "Google Chrome Blog: Faster than fast" (http://chrome.blogspot.com/2011/06/faster-than-fast.html). chrome.blogspot.com. Retrieved August 21, 2011.

25. "Building better web apps with a new Chrome Beta" (http://chrome.blogspot.com/2011/08/building-better-web-apps-with-new.html). Retrieved August 15, 2011.

26. Langley, Adam (August 16, 2010). "DNSSEC authenticated HTTPS in Chrome" (http://www.imperialviolet.org/2011/06/16/dnssecchrome.html). ImperialViolet. Retrieved April 8, 2012.

27. "Chrome Beta Channel Update" (http://googlechromereleases.blogspot.com/2011/08/chrome-beta-channel-update.html). Retrieved August 15, 2011.

28. "Download Google Chrome 15.0.874.15 Dev with Fixes for the Revamped New Tab Page" (http://news.softpedia.com/news/Download-Google-Chrome-15-0-874-15-Dev-with-Fixes-for-the-Revamped-New-Tab-Page-222051.shtml). Retrieved September 19, 2011.

29. "Download Google Chrome 16 Dev and Chrome 15 Beta" (http://news.softpedia.com/news/Download-Google-Chrome-16-Dev-and-Chrome-15-Beta-223218.shtml). Retrieved September 23, 2011.

30. "Issue 50811 – chromium – Switch Chromium to ffmpeg native vp8 decoder – An open-source browser project to help move the web forward. – Google Project Hosting" (https://code.google.com/p/chromium/issues/detail?id=50811). July 30, 2010. Retrieved April 8, 2012.

31. "Issue 48119: Feature request: optional permissions in Chrome extensions" (https://code.google.com/p/chromium/issues/detail?id=48119). *Chromium Bugs*. July 1, 2010. Retrieved February 4, 2012.

32. "Issue 99332: Remove sidetabs" (https://code.google.com/p/chromium/issues/detail?id=99332). *Chromium Bugs*. October 6, 2011. Retrieved February 4, 2012.

33. "Stable Channel Update" (http://googlechromereleases.blogspot.com/2012/02/stable-channel-update.html). Retrieved February 9, 2012.

34. "Google Chrome 17 FINAL" (https://web.archive.org/web/20120206190947/http://www.downloadcrew.com/article/23259-google_chrome_stable). Archived from the original (http://www.downloadcrew.com/article/23259-google_chrome_stable) on February 6, 2012. Retrieved February 9, 2012.

35. "Chromium Issue 15548: Search Engines should be synced" (https://code.google.com/p/chromium/issues/detail?id=15548). June 28, 2009. Retrieved April 8, 2012.

36. Ilascu, Ionut (January 19, 2012). "Google Chrome Beta 17.0.963.38 Disables GAIA Photo" (http://news.softpedia.com/news/Google-Chrome-Beta-17-0-963-38-Disables-GAIA-Photo-247483.shtml). Softpedia. Retrieved December 27, 2012.

37. "Faster graphics for older PCs in Chrome 18" (https://web.archive.org/web/20120509104031/http://download.cnet.com/8301-2007_4-57405953-12/faster-graphics-for-older-pcs-in-chrome-18/). Archived from the original (http://download.cnet.com/8301-2007_4-57405953-12/faster-graphics-for-older-pcs-in-chrome-18) on May 9, 2012. Retrieved June 25, 2013.

38. "[chrome] Revision 119099" (https://src.chromium.org/viewvc/chrome?view=rev&revision=119099). Src.chromium.org. Retrieved May 23, 2012.

39. "Google Chrome Blog: All your tabs, accessible everywhere" (http://chrome.blogspot.com.au/2012/04/all-your-tabs-accessible-everywhere.html). chrome.blogspot.com.au. April 10, 2012. Retrieved May 23, 2012.

40. "Google Chrome 19 Adds Support for Next-Generation JavaScript" (http://news.softpedia.com/news/Google-Chrome-19-Adds-Support-for-Next-Generation-JavaScript-252219.shtml). Softpedia. February 11, 2012. Retrieved May 15, 2012.

41. "Connect with Web Intents" (https://blog.chromium.org/2012/05/connect-with-web-intents.html). May 16, 2012. Retrieved May 16, 2012.

42. "[chrome] Revision 133210]" (https://src.chromium.org/viewvc/chrome?view=rev&revision=133210).

43. "Decreased input padding, 8-bit canvas and getUserMedia() « Peter Beverloo" (http://peter.sh/2012/05/decreased-input-padding-8-bit-canvas-and-getusermedia/). Peter Beverloo. Retrieved May 23, 2012.

44. "Dev Channel Update" (http://googlechromereleases.blogspot.com/2012/05/dev-channel-update_29.html). May 29, 2012. Retrieved June 1, 2011.

45. "Stable Channel Update" (http://googlechromereleases.blogspot.com/2012/08/stable-channel-update_21.html). August 21, 2012. Retrieved August 22, 2012.

46. "Issue 143: Handle color profiles in tagged images" (https://code.google.com/p/chromium/issues/detail?id=143). September 2, 2008. Retrieved March 23, 2013.

47. Bright, Peter (September 14, 2012). "Do Not Track support added to Chrome, arriving by the end of the year" (https://arstechnica.com/information-technology/2012/09/do-not-track-support-added-to-chrome-arriving-by-the-end-of-the-year/). *Ars Technica*. Retrieved November 2, 2012.

48. "Securing Flash Player for our Mac users" (http://chrome.blogspot.com/2012/11/securing-flash-player-for-our-mac-users.html). Retrieved November 14, 2012.

49. "A web developer's guide to t11-08" (https://blog.chromium.org/2012/11/a-web-developers-guide-to-latest-chrome.html). Retrieved November 9, 2012.

50. "CSS Custom Filters" (https://adobe.github.com/web-platform/samples/css-customfilters/). Adobe.github.com. Retrieved March 23, 2013.

51. Hewitt, Ed (February 21, 2013). "Google Chrome hits 25" (http://www.omgchrome.com/google-chrome-hits-25/). OMG! Chrome!. Retrieved March 23, 2013.

52. "No more silent extension installs" (https://blog.chromium.org/2012/12/no-more-silent-extension-installs.html). Chromium Blog. December 24, 2012. Retrieved December 24, 2012.

53. "Chrome 25 Beta: Content Security Policy and Shadow DOM" (https://blog.chromium.org/2013/01/content-security-policy-and-shadow-dom.html). Chromium Blog. January 14, 2013. Retrieved January 19, 2013.

54. "Google Search in Chrome gets more secure" (https://blog.chromium.org/2013/01/google-search-in-chrome-gets-more-secure.html). Chromium Blog. January 18, 2013. Retrieved January 19, 2013.

55. "Issue 174455: MathML support broken with Chrome 25 beta" (https://code.google.com/p/chromium/issues/detail?id=174455#c2). February 5, 2013. Retrieved February 19, 2013.

56. Govindan, Dharani (March 26, 2013). "Stable Channel Update" (http://googlechromereleases.blogspot.com/2013/03/stable-channel-update_26.html). *Chrome Releases*. Blogger. Retrieved March 26, 2013.

57. "Google Chrome Blog: Fill out forms faster, from anywhere" (http://chrome.blogspot.com/2013/04/fill-out-forms-faster-from-anywhere.html).

58. "Chrome Release: Stable Channel Release" (http://googlechromereleases.blogspot.com/2013/05/stable-channel-release.html). May 21, 2013. Retrieved May 22, 2013.

59. "Manifest Version - Google Chrome" (https://developer.chrome.com/extensions/manifestVersion.html). Developer.chrome.com. March 4, 2013. Retrieved March 30, 2013.

60. "Chrome Releases: Chrome for Android Update" (http://googlechromereleases.blogspot.com/2013/05/chrome-for-android-update.html).

61. Protalinski, Emil (April 4, 2013). "Google's Blink Q&A: New rendering engine will replace WebKit on all platforms in 10 weeks with Chrome 28" (https://thenextweb.com/google/2013/04/04/googles-blink-qa-new-rendering-engine-will-replace-webkit-on-all-platforms-in-10-weeks-with-chrome-28/). The Next Web. Retrieved April 5, 2013.

62. Shankland, Stephen. "Blink, Google's new Chrome browser engine, comes to life" (http://news.cnet.com/8301-17939_109-57577922-2/blink-googles-new-chrome-browser-engine-comes-to-life/). *CNET News*. CNET. Retrieved April 5, 2013.

63. Finley, Klint. "Google Chrome Breaks Up With Apple's WebKit" (https://www.wired.com/wiredenterprise/2013/04/blink/). *Wired Enterprise*. Retrieved April 5, 2013.

64. "Chrome 28 Beta: A more immersive web, everywhere" (https://blog.chromium.org/2013/05/chrome-28-beta-more-immersive-web.html). Retrieved June 17, 2013.

65. Protalinski, Emil (May 23, 2013). "Google debuts Chrome 28 beta with rich notifications for apps and extensions on Windows; Mac and Linux coming soon" (https://thenextweb.com/google/2013/05/23/google-debuts-chrome-28-beta-with-rich-notifications-for-apps-and-extensions-on-windows-coming-to-os-x-next/). The Next Web. Retrieved June 17, 2013.

66. "Google Chrome Blog: More multilingual mobile web" (http://chrome.blogspot.hu/2013/07/more-multilingual-mobile-web.html). Retrieved July 11, 2013.

67. "Chrome Releases: Chrome for iOS Update" (http://googlechromereleases.blogspot.hu/2013/07/chrome-for-ios-update.html).

68. "Chromium Code Reviews: Issue 12317026: Various small QUIC cleanups after merging to Chrome" (https://chromiumcodereview.appspot.com/12317026/). Retrieved February 22, 2013.

69. "Connecting Chrome apps and extensions with native applications" (https://blog.chromium.org/2013/10/connecting-chrome-apps-and-extensions.html). October 15, 2013. Retrieved October 24, 2015.

70. "Chrome for Android Update - WebRTC support" (http://googlechromereleases.blogspot.hu/2013/08/chrome-for-android-update.html).

71. "The Next Web: Chrome 29 for Android is out: WebRTC and Web Audio support, improved scrolling, and new color picker for Web forms" (https://thenextweb.com/google/2013/08/21/chrome-29-for-android-is-out-webrtc-and-webaudio-support-improved-scrolling-and-new-color-picker-for-web-forms). August 21, 2013.

72. "Chrome for iOS Update" (http://googlechromereleases.blogspot.hu/2013/09/chrome-for-ios-update.html).

73. "Chrome for iOS Gets 'Conversational Search' " (http://www.chromestory.com/2013/09/chrome-ios-gets-conversational-search/). *Chrome Story*. September 13, 2013.

74. "Chromium Blog: Chrome 30 Beta: A richer web on Android" (https://blog.chromium.org/2013/08/chrome-30-beta-richer-web-on-android.html). *Chromium Blog*.

75. "Chrome for iOS Update" (https://itunes.apple.com/us/app/chrome/id535886823).

76. "Chromium Blog: Chrome 31 Beta: Android Application Shortcuts, requestAutocomplete(), and PNaCl" (https://blog.chromium.org/2013/10/chrome-31-beta-android-application.html). *Chromium Blog*.

77. "Chrome Releases: Chrome for Android Update" (http://googlechromereleases.blogspot.hu/2014/01/chrome-for-android-update.html). *Chrome Releases*.

78. "Chromium Dashboard" (https://www.chromestatus.com/features). Retrieved March 9, 2014.

79. "Chrome Releases" (http://googlechromereleases.blogspot.se/).

80. "Deprecation Info Bar for Chrome 34 users" (https://codereview.chromium.org/193493005). Chromium Code Review. Retrieved April 4, 2022.

81. "Stable Channel Update" (http://googlechromereleases.blogspot.com/2014/07/stable-channel-update.html).

82. "Chrome for Android Update" (http://googlechromereleases.blogspot.com/2014/07/chrome-for-android-update.html).

83. "Chrome for iOS Update" (http://googlechromereleases.blogspot.com/2014/07/chrome-for-ios-update.html).

84. "Stable Channel Update" (http://googlechromereleases.blogspot.com/2014/08/stable-channel-update_26.html).

85. "Chrome's Lack of Support for showModalDialog Breaks Some Enterprise Web Apps" (http://www.infoq.com/news/2014/09/chrome-showmodaldialog). *InfoQ*.

86. "Chrome for Android Update" (http://googlechromereleases.blogspot.com/2014/09/chrome-for-android-update.html). September 3, 2014. Retrieved September 3, 2014.

87. "64 bits of awesome: 64-bit Windows Support, now in Stable!" (https://blog.chromium.org/2014/08/64-bits-of-awesome-64-bit-windows_26.html). August 26, 2014. Retrieved August 27, 2014.

88. "Google beefs up 2-step verification with physical USB Security Key option in Chrome" (https://venturebeat.com/2014/10/21/google-beefs-up-2-step-verification-with-physical-usb-security-key-option-in-chrome/). October 21, 2014. Retrieved October 24, 2014.

89. "Stable Channel Release" (http://googlechromereleases.blogspot.com/2014/10/stable-channel-update.html). October 7, 2014. Retrieved October 7, 2014.

90. "Chrome for Android Update" (http://googlechromereleases.blogspot.com/2014/10/chrome-for-android-update.html). October 8, 2014. Retrieved October 8, 2014.

91. "Chrome for iOS Update" (http://googlechromereleases.blogspot.com/2014/10/chrome-for-ios-update.html). October 7, 2014. Retrieved October 7, 2014.

92. "Stable Channel Release" (http://googlechromereleases.blogspot.com/2014/11/stable-channel-update_18.html). November 18, 2014. Retrieved November 18, 2014.

93. "Chrome for Android Update" (http://googlechromereleases.blogspot.com/2014/11/chrome-for-android-update.html). November 12, 2014. Retrieved November 12, 2014.

94. "Google Chrome Beta Updated To v39 With Reader Mode And Tweaked Tab Closing Animation" (http://www.androidpolice.com/2014/10/14/google-chrome-beta-updated-to-v39-with-reader-mode-and-tweaked-tab-closing-animation-apk-download/). October 14, 2014. Retrieved November 14, 2014.

95. "Stable Channel Release" (http://googlechromereleases.blogspot.com/2015/01/stable-update.html). January 21, 2015. Retrieved January 21, 2015.

96. "Chrome for Android Update" (http://googlechromereleases.blogspot.com/2015/01/chrome-for-android-update.html). January 21, 2015. Retrieved January 21, 2015.

97. "Chrome for iOS Update" (http://googlechromereleases.blogspot.com/2015/01/chrome-for-ios-update.html). January 20, 2015. Retrieved January 20, 2015.

98. "Stable Channel Update" (http://googlechromereleases.blogspot.com/2015/03/stable-channel-update.html). March 3, 2015. Retrieved March 3, 2015.

99. "Chrome for Android Update" (http://googlechromereleases.blogspot.com/2015/03/chrome-for-android-update.html). March 11, 2015. Retrieved March 11, 2015.

100. "Stable Channel Update" (http://googlechromereleases.blogspot.com/2015/04/stable-channel-update_14.html). April 14, 2015. Retrieved April 14, 2015.

101. "Chrome for Android Update" (http://googlechromereleases.blogspot.com/2015/04/chrome-for-android-update.html). April 15, 2015. Retrieved April 15, 2015.

102. "Stable Channel Update" (http://googlechromereleases.blogspot.com/2015/05/stable-channel-update_19.html). May 19, 2015. Retrieved May 19, 2015.

103. "Chrome for Android Update" (http://googlechromereleases.blogspot.com/2015/05/chrome-for-android-update.html). May 27, 2015. Retrieved May 27, 2015.

104. Brinkmann, Martin (March 3, 2015). "You need to stop using Chrome on Android 4.0 Ice Cream Sandwich - gHacks Tech News" (http://www.ghacks.net/2015/03/03/you-need-to-stop-using-chrome-on-android-4-0-ice-cream-sandwich/). *gHacks Technology News*. Retrieved August 31, 2015.

105. Tung, Liam (March 4, 2015). "Google to ditch Chrome support for Android 4.0 Ice Cream Sandwich" (https://www.zdnet.com/article/google-to-ditch-chrome-support-for-android-4-0-ice-cream-sandwich/). *ZDNet*. Retrieved August 31, 2015.

106. "Stable Channel Update" (http://googlechromereleases.blogspot.com/2015/07/stable-channel-update_21.html). July 21, 2015. Retrieved July 21, 2015.

107. "Chrome for Android Update" (http://googlechromereleases.blogspot.com/2015/07/chrome-for-android-update.html). July 29, 2015. Retrieved July 29, 2015.

108. "Chrome for iOS Update" (http://googlechromereleases.blogspot.com/2015/07/chrome-for-ios-update.html). July 22, 2015. Retrieved July 22, 2015.

109. "Stable Channel Update" (http://googlechromereleases.blogspot.com/2015/09/stable-channel-update.html). September 1, 2015. Retrieved September 1, 2015.

110. "Chrome for Android Update" (http://googlechromereleases.blogspot.com/2015/09/chrome-for-android-update.html). September 1, 2015. Retrieved September 1, 2015.

111. "Stable Channel Update" (http://googlechromereleases.blogspot.com/2015/10/stable-channel-update.html). October 13, 2015. Retrieved October 13, 2015.

112. "Chrome for Android Update" (http://googlechromereleases.blogspot.com/2015/10/chrome-for-android-update.html). October 14, 2015. Retrieved October 15, 2015.

113. "Stable Channel Update" (http://googlechromereleases.blogspot.ca/2015/12/stable-channel-update.html). December 1, 2015. Retrieved December 1, 2015.

114. "Chrome for Android Update" (http://googlechromereleases.blogspot.com/2015/12/chrome-for-android-update.html). December 2, 2015. Retrieved December 3, 2015.

115. "Stable Channel Update" (http://googlechromereleases.blogspot.com/2016/01/stable-channel-update_20.html). January 20, 2016. Retrieved January 20, 2016.

116. "Stable Channel Update" (http://googlechromereleases.blogspot.com/2016/03/stable-channel-update.html). March 2, 2016. Retrieved March 2, 2016.

117. "Chrome for Android Update" (http://googlechromereleases.blogspot.com/2016/03/chrome-for-android-update.html). March 9, 2016. Retrieved March 9, 2016.

118. "Stable Channel Update" (http://googlechromereleases.blogspot.com/2016/04/stable-channel-update_13.html). April 13, 2016. Retrieved April 13, 2016.

119. "Stable Channel Update" (http://googlechromereleases.blogspot.com/2016/05/stable-channel-update_25.html). May 25, 2016. Retrieved May 25, 2016.

120. "Chrome for Android Update" (https://googlechromereleases.blogspot.com/2016/06/chrome-for-android-update.html). June 7, 2016. Retrieved September 10, 2016.

121. "Stable Channel Update" (http://googlechromereleases.blogspot.com/2016/07/stable-channel-update.html). July 20, 2016. Retrieved July 20, 2016.

122. "Chrome for Android Update" (http://googlechromereleases.blogspot.com/2016/07/chrome-for-android-update.html). July 27, 2016. Retrieved July 28, 2016.

123. "Stable Channel Update for Desktop" (https://googlechromereleases.blogspot.com/2016/08/stable-channel-update-for-desktop_31.html). August 31, 2016. Retrieved August 31, 2016.

124. "Chrome for Android Update" (https://googlechromereleases.blogspot.com/2016/09/chrome-for-android-update.html). *Chrome Releases*. September 7, 2016. Retrieved September 8, 2016.

125. "Muted Autoplay on Mobile: Say Goodbye to Canvas Hacks and Animated GIFs!" (https://developers.google.com/web/updates/2016/07/autoplay). *Google Developers*. Retrieved November 3, 2016.

126. "Stable Channel Update for Desktop" (https://googlechromereleases.blogspot.com/2016/10/stable-channel-update-for-desktop.html). October 12, 2016. Retrieved October 12, 2016.

127. "Chrome for Android Update" (https://googlechromereleases.blogspot.com/2016/10/chrome-for-android-update.html). October 19, 2016. Retrieved October 20, 2016.

128. "Stable Channel Update for Desktop" (https://googlechromereleases.blogspot.com/2016/12/stable-channel-update-for-desktop.html). December 1, 2016. Retrieved December 2, 2016.

129. "Google removes the 'Material Design in the browser's top Chrome' flag | Techdows" (http://techdows.com/2016/09/material-design-in-the-browsers-top-chrome-flag-removed.html). *techdows.com*.

130. "Chrome for Android Update" (https://googlechromereleases.blogspot.com/2016/12/chrome-for-android-update.html). December 6, 2016. Retrieved December 7, 2016.

131. "Stable Channel Update for Desktop" (https://chromereleases.googleblog.com/2017/01/stable-channel-update-for-desktop.html). January 25, 2017. Retrieved January 26, 2017.

132. "Chrome for Android Update" (https://chromereleases.googleblog.com/2017/02/chrome-for-android-update.html). February 1, 2017. Retrieved February 2, 2017.

133. "Stable Channel Update for Desktop" (https://chromereleases.googleblog.com/2017/03/stable-channel-update-for-desktop.html). March 9, 2017. Retrieved March 9, 2017.

134. "Chrome 57 Beta: CSS Grid Layout, Improved Add to Home screen, Media Session API" (https://blog.chromium.org/2017/02/chrome-57-beta-css-grid-layout-improved.html). February 2, 2017.

135. "Chrome for Android Update" (https://chromereleases.googleblog.com/2017/03/chrome-for-android-update.html). March 16, 2017. Retrieved March 17, 2017.

136. "Stable Channel Update for Desktop" (https://chromereleases.googleblog.com/2017/04/stable-channel-update-for-desktop.html). April 19, 2017. Retrieved April 19, 2017.

137. "Chrome for Android Update" (https://chromereleases.googleblog.com/2017/04/chrome-for-android-update.html). April 25, 2017. Retrieved April 26, 2017.

138. "Stable Channel Update for Desktop" (https://chromereleases.googleblog.com/2017/06/stable-channel-update-for-desktop.html). June 5, 2017. Retrieved June 6, 2017.

139. LePage, Pete (May 2017). "New in Chrome 59" (https://developers.google.com/web/updates/2017/05/nic59). Google Inc. Retrieved June 10, 2017.

140. "Chrome for Android Update" (https://chromereleases.googleblog.com/2017/06/chrome-for-android-update.html). June 6, 2017. Retrieved June 7, 2017.

141. "Stable Channel Update for Desktop" (https://chromereleases.googleblog.com/2017/07/stable-channel-update-for-desktop.html). July 25, 2017. Retrieved July 25, 2017.

142. "Chrome for Android Update" (https://chromereleases.googleblog.com/2017/08/chrome-for-android-update.html). August 1, 2017. Retrieved August 2, 2017.

143. "Stable Channel Update for Desktop" (https://chromereleases.googleblog.com/2017/09/stable-channel-update-for-desktop.html). September 5, 2017. Retrieved September 5, 2017.

144. "Chrome for Android Update" (https://chromereleases.googleblog.com/2017/09/chrome-for-android-update.html). September 5, 2017. Retrieved September 6, 2017.

145. "Stable Channel Update for Desktop" (https://chromereleases.googleblog.com/2017/10/stable-channel-update-for-desktop.html). October 17, 2017. Retrieved October 18, 2017.

146. "New in Chrome 62" (https://developers.google.com/web/updates/2017/10/nic62). Google Inc. Retrieved October 18, 2017.

147. "Chrome for Android Update" (https://chromereleases.googleblog.com/2017/10/chrome-for-android-update.html). October 24, 2017. Retrieved October 24, 2017.

148. "Stable Channel Update for Desktop" (https://chromereleases.googleblog.com/2017/12/stable-channel-update-for-desktop.html). December 6, 2017. Retrieved December 6, 2017.

149. "New in Chrome 63" (https://developers.google.com/web/updates/2017/12/nic63). Google Inc. Retrieved December 14, 2017.

150. "Chrome for Android Update" (https://chromereleases.googleblog.com/2017/12/chrome-for-android-update.html). December 5, 2017. Retrieved December 6, 2017.

151. "Stable Channel Update for Desktop" (https://chromereleases.googleblog.com/2018/01/stable-channel-update-for-desktop_24.html). January 24, 2018. Retrieved January 24, 2018.

152. "New in Chrome 64" (https://developers.google.com/web/updates/2018/01/nic64). Google Inc. Retrieved January 25, 2018.

153. "Convert CRX creator to create CRX3 items" (https://chromium.googlesource.com/chromium/src.git/+/b8bc9f99ef4ad6223dfdcafd924051561c05ac75). Chromium Google Source. Retrieved March 31, 2019.

154. "Chrome for Android Update" (https://chromereleases.googleblog.com/2018/01/chrome-for-android-update.html). January 23, 2018. Retrieved January 24, 2018.

155. "Stable Channel Update for Desktop" (https://chromereleases.googleblog.com/2018/03/stable-channel-update-for-desktop.html). March 6, 2018. Retrieved March 6, 2018.

156. "New in Chrome 65" (https://developers.google.com/web/updates/2018/03/nic65). Google Inc. Retrieved March 6, 2018.

157. "Chrome for Android Update" (https://chromereleases.googleblog.com/2018/03/chrome-for-android-update.html). *Chrome Releases*. March 6, 2018. Retrieved March 6, 2018.

158. "Stable Channel Update for Desktop" (https://chromereleases.googleblog.com/2018/04/stable-channel-update-for-desktop.html). April 17, 2018. Retrieved April 18, 2018.

159. "New in Chrome 66" (https://developers.google.com/web/updates/2018/04/nic66). Google Inc. Retrieved April 18, 2018.

160. "Chrome for Android Update" (https://chromereleases.googleblog.com/2018/04/chrome-for-android-update.html). April 17, 2018. Retrieved April 18, 2018.

161. "Stable Channel Update for Desktop" (https://chromereleases.googleblog.com/2018/05/stable-channel-update-for-desktop_58.html). May 29, 2018. Retrieved May 29, 2018.

162. "New in Chrome 67" (https://developers.google.com/web/updates/2018/05/nic67). Google Inc. Retrieved May 29, 2018.

163. "Chrome for Android Update" (https://chromereleases.googleblog.com/2018/05/chrome-for-android-update_31.html). May 31, 2018. Retrieved May 31, 2018.

164. "Stable Channel Update for Desktop" (https://chromereleases.googleblog.com/2018/07/stable-channel-update-for-desktop_58.html). July 24, 2018. Retrieved July 24, 2018.

165. "New in Chrome 68" (https://developers.google.com/web/updates/2018/07/nic68). Google Inc. Retrieved July 24, 2018.

166. "Chrome for Android Update" (https://chromereleases.googleblog.com/2018/07/chrome-for-android-update.html). July 24, 2018. Retrieved July 25, 2018.

167. "Stable Channel Update for Desktop" (https://chromereleases.googleblog.com/2018/09/stable-channel-update-for-desktop.html). September 4, 2018. Retrieved September 4, 2018.

168. "New in Chrome 69" (https://developers.google.com/web/updates/2018/09/nic69). Google Inc. Retrieved September 4, 2018.

169. "Chrome for Android Update" (https://chromereleases.googleblog.com/2018/09/chrome-for-android-update.html). September 4, 2018. Retrieved September 4, 2018.

170. "Stable Channel Update for Desktop" (https://chromereleases.googleblog.com/2018/10/stable-channel-update-for-desktop.html). October 16, 2018. Retrieved October 16, 2018.

171. "Audio/Video Updates in Chrome 70" (https://developers.google.com/web/updates/2018/09/chrome-70-media-updates). Google Inc. Retrieved September 18, 2018.

172. "Deprecations and removals in Chrome 70" (https://developers.google.com/web/updates/2018/09/chrome-70-deps-rems). Google Inc. Retrieved October 16, 2018.

173. "Chrome for Android Update" (https://chromereleases.googleblog.com/2018/10/chrome-for-android-update.html). October 17, 2018. Retrieved October 17, 2018.

174. "Stable Channel Update for Desktop" (https://chromereleases.googleblog.com/2018/12/stable-channel-update-for-desktop.html). December 4, 2018. Retrieved December 4, 2018.

175. "New in Chrome 71" (https://developers.google.com/web/updates/2018/12/nic71). Google Inc. Retrieved December 4, 2018.

176. "Deprecations and removals in Chrome 71" (https://developers.google.com/web/updates/2018/10/chrome-71-deps-rems). Google Inc. Retrieved December 4, 2018.

177. "Chrome for Android Update" (https://chromereleases.googleblog.com/2018/12/chrome-for-android-update.html). December 4, 2018. Retrieved December 5, 2018.

178. "Stable Channel Update for Desktop" (https://chromereleases.googleblog.com/2019/01/stable-channel-update-for-desktop.html). January 29, 2019. Retrieved January 29, 2019.

179. "New in Chrome 72" (https://developers.google.com/web/updates/2019/01/nic72). Google Inc. Retrieved January 29, 2019.

180. "Deprecations and removals in Chrome 72" (https://developers.google.com/web/updates/2018/12/chrome-72-deps-rems). Google Inc. Retrieved January 29, 2019.

181. "Chrome for Android Update" (https://chromereleases.googleblog.com/2019/01/chrome-for-android-update_29.html). January 29, 2019. Retrieved January 29, 2019.

182. "Stable Channel Update for Desktop" (https://chromereleases.googleblog.com/2019/03/stable-channel-update-for-desktop_12.html). March 12, 2019. Retrieved March 12, 2019.

183. "New in Chrome 73" (https://developers.google.com/web/updates/2019/03/nic73). Google Inc. Retrieved March 12, 2019.

184. "Deprecations and removals in Chrome 73" (https://developers.google.com/web/updates/2019/02/chrome-73-deps-rems). Google Inc. Retrieved March 12, 2019.

185. "External CRXs must be crx3s" (https://chromium.googlesource.com/chromium/src/+/77bc0247a52ab0bb9c4b405a6a790aa0f034edcc). Chromium Google Source. Retrieved March 31, 2019.

186. "Chrome for Android Update" (https://chromereleases.googleblog.com/2019/03/chrome-for-android-update_12.html). March 12, 2019. Retrieved March 12, 2019.

187. "Stable Channel Update for Desktop" (https://chromereleases.googleblog.com/2019/04/stable-channel-update-for-desktop_23.html). April 23, 2019. Retrieved April 23, 2019.

188. "New in Chrome 74" (https://developers.google.com/web/updates/2019/04/nic74). Google Inc. Retrieved April 23, 2019.

189. "Deprecations and removals in Chrome 74" (https://developers.google.com/web/updates/2019/03/chrome-74-deps-rems). Google Inc. Retrieved April 23, 2019.

190. "Chrome for Android Update" (https://chromereleases.googleblog.com/2019/04/chrome-for-android-update.html). April 24, 2019. Retrieved April 25, 2019.

191. "Stable Channel Update for Desktop" (https://chromereleases.googleblog.com/2019/06/stable-channel-update-for-desktop.html). June 4, 2019. Retrieved June 4, 2019.

192. "New in Chrome 75" (https://developers.google.com/web/updates/2019/06/nic75). Google Inc. Retrieved July 30, 2019.

193. "Deprecations and removals in Chrome 75" (https://developers.google.com/web/updates/2019/05/chrome-75-deps-rems). Google Inc. Retrieved June 4, 2019.

194. "Chrome for Android Update" (https://chromereleases.googleblog.com/2019/06/chrome-for-android-update.html). June 4, 2019. Retrieved June 5, 2019.

195. "Stable Channel Update for Desktop" (https://chromereleases.googleblog.com/2019/07/stable-channel-update-for-desktop_30.html). July 30, 2019. Retrieved July 30, 2019.

196. "New in Chrome 76" (https://developers.google.com/web/updates/2019/07/nic76). Google Inc. Retrieved July 30, 2019.

197. "Deprecations and removals in Chrome 76" (https://developers.google.com/web/updates/2019/06/chrome-76-deps-rems). Google Inc. Retrieved July 30, 2019.

198. "Chrome for Android Update" (https://chromereleases.googleblog.com/2019/07/chrome-for-android-update_30.html). July 30, 2019. Retrieved July 31, 2019.

199. "Stable Channel Update for Desktop" (https://chromereleases.googleblog.com/2019/09/stable-channel-update-for-desktop.html). September 10, 2019. Retrieved September 10, 2019.

200. "New in Chrome 77" (https://developers.google.com/web/updates/2019/09/nic77). Google Inc. Retrieved September 19, 2019.

201. "Deprecations and removals in Chrome 77" (https://developers.google.com/web/updates/2019/08/chrome-77-deps-rems). Google Inc. Retrieved September 10, 2019.

202. "Chrome for Android Update" (https://chromereleases.googleblog.com/2019/09/chrome-for-android-update.html). September 10, 2019. Retrieved September 10, 2019.

203. "Stable Channel Update for Desktop" (https://chromereleases.googleblog.com/2019/10/stable-channel-update-for-desktop_22.html). October 22, 2019. Retrieved October 22, 2019.

204. "New in Chrome 78" (https://developers.google.com/web/updates/2019/10/nic78). Google Inc. Retrieved October 22, 2019.

205. "Deprecations and removals in Chrome 78" (https://developers.google.com/web/updates/2019/09/chrome-78-deps-rems). Google Inc. Retrieved October 22, 2019.

206. "Chrome for Android Update" (https://chromereleases.googleblog.com/2019/10/chrome-for-android-update_22.html). October 22, 2019. Retrieved October 22, 2019.

207. "Stable Channel Update for Desktop" (https://chromereleases.googleblog.com/2019/12/stable-channel-update-for-desktop.html). December 10, 2019. Retrieved December 10, 2019.

208. "New in Chrome 79" (https://developers.google.com/web/updates/2019/12/nic79). Google Inc. Retrieved December 10, 2019.

209. "Deprecations and removals in Chrome 79 [numbering mislabeled as "Chrome 78"]" (https://developers.google.com/web/updates/2019/10/chrome-79-deps-rems). Google Inc. Retrieved December 10, 2019.

210. "Chrome for Android Update" (https://chromereleases.googleblog.com/2019/12/chrome-for-android-update.html). December 10, 2019. Retrieved December 11, 2019.

211. "Stable Channel Update for Desktop" (https://chromereleases.googleblog.com/2020/02/stable-channel-update-for-desktop.html). February 4, 2020. Retrieved February 4, 2020.

212. "New in Chrome 80" (https://developers.google.com/web/updates/2020/02/nic80). Google Inc. Retrieved February 5, 2020.

213. "Deprecations and removals in Chrome 80" (https://developers.google.com/web/updates/2019/12/chrome-80-deps-rems). Google Inc. Retrieved February 4, 2020.

214. "Chrome for Android Update" (https://chromereleases.googleblog.com/2020/02/chrome-for-android-update.html). February 4, 2020. Retrieved February 5, 2020.

Case 4:20-cv-03664-YGR   Document 928-20   Filed 04/19/23   Page 389 of 405

215. "Stable Channel Update for Desktop" (https://chromereleases.googleblog.com/2020/04/stable-channel-update-for-desktop_7.html)
. April 7, 2020. Retrieved April 7, 2020.

216. "New in Chrome 81" (https://developers.google.com/web/updates/2020/04/nic81). Google Inc. Retrieved April 7, 2020.

217. "Deprecations and removals in Chrome 80" (https://developers.google.com/web/updates/2020/02/chrome-81-deps-rems). Google
Inc. Retrieved February 4, 2020.

218. "Chrome for Android Update" (https://chromereleases.googleblog.com/2020/04/chrome-for-android-update.html). April 7, 2020.
Retrieved April 7, 2020.

219. "Stable Channel Update for Desktop" (https://chromereleases.googleblog.com/2020/05/stable-channel-update-for-desktop_19.htm
l). May 19, 2020. Retrieved May 19, 2020.

220. "New in Chrome 83" (https://developers.google.com/web/updates/2020/05/nic83). Google Inc. Retrieved May 19, 2020.

221. "Deprecations and removals in Chrome 83" (https://developers.google.com/web/updates/2020/04/chrome-83-deps-rems). Google
Inc. Retrieved May 19, 2020.

222. "Android KitKat will soon be deprecated in the Chromium code base" (https://groups.google.com/a/chromium.org/forum/m/#!topic/
chromium-dev/ypAS49lvN1M). Google Groups. January 14, 2020. Retrieved January 14, 2020.

223. "Chrome for Android Update" (https://chromereleases.googleblog.com/2020/05/chrome-for-android-update_19.html). May 19,
2020. Retrieved May 19, 2020.

224. "Stable Channel Update for Desktop" (https://chromereleases.googleblog.com/2020/07/stable-channel-update-for-desktop.html).
July 14, 2020. Retrieved July 14, 2020.

225. "New in Chrome 84" (https://developers.google.com/web/updates/2020/07/nic84). Google Inc. Retrieved July 14, 2020.

226. "Deprecations and removals in Chrome 84" (https://developers.google.com/web/updates/2020/05/chrome-84-deps-rems). Google
Inc. Retrieved July 14, 2020.

227. "Chrome for Android Update" (https://chromereleases.googleblog.com/2020/07/chrome-for-android-update_14.html). July 14,
2020. Retrieved July 15, 2020.

228. "Chrome for iOS Update" (https://chromereleases.googleblog.com/2020/07/chrome-for-ios-update.html). July 14, 2020. Retrieved
July 14, 2020.

229. "Stable Channel Update for Desktop" (https://chromereleases.googleblog.com/2020/08/stable-channel-update-for-desktop_25.htm
l). August 25, 2020. Retrieved August 25, 2020.

230. "Deprecations and removals in Chrome 85" (https://developers.google.com/web/updates/2020/07/chrome-85-deps-rems). Google
Inc. Retrieved August 25, 2020.

231. "Chrome for iOS Update" (https://chromereleases.googleblog.com/2020/08/chrome-for-ios-update.html). August 25, 2020.
Retrieved August 25, 2020.

232. "Chrome for Android Update" (https://chromereleases.googleblog.com/2020/08/chrome-for-android-update.html). August 25,
2020. Retrieved August 26, 2020.

233. "Stable Channel Update for Desktop" (https://chromereleases.googleblog.com/2020/10/stable-channel-update-for-desktop.html).
October 6, 2020. Retrieved October 7, 2020.

234. "New in Chrome 86" (https://developers.google.com/web/updates/2020/10/nic86). Google Inc. Retrieved October 6, 2020.

235. "Deprecations and removals in Chrome 86" (https://developers.google.com/web/updates/2020/09/chrome-86-deps-rems). Google
Inc. Retrieved October 6, 2020.

236. "Chrome for Android Update" (https://chromereleases.googleblog.com/2020/10/chrome-for-android-update.html). October 6, 2020.
Retrieved October 7, 2020.

237. "Stable Channel Update for Desktop" (https://chromereleases.googleblog.com/2020/11/stable-channel-update-for-desktop_17.htm
l). November 17, 2020. Retrieved November 18, 2020.

238. "New in Chrome 87" (https://developers.google.com/web/updates/2020/11/nic87). Google Inc. Retrieved November 18, 2020.

239. "Deprecations and removals in Chrome 87" (https://developers.google.com/web/updates/2020/10/chrome-87-deps-rems). Google
Inc. Retrieved November 18, 2020.

240. "Chrome for Android Update" (https://chromereleases.googleblog.com/2020/11/chrome-for-android-update_17.html). November
17, 2020. Retrieved November 18, 2020.

241. "Chrome for iOS Update" (https://chromereleases.googleblog.com/2020/11/chrome-for-ios-update.html). November 18, 2020.
Retrieved November 19, 2020.

242. "Stable Channel Update for Desktop" (https://chromereleases.googleblog.com/2021/01/stable-channel-update-for-desktop_19.htm
l). January 19, 2021. Retrieved January 19, 2021.

243. "New in Chrome 88" (https://developers.google.com/web/updates/2021/01/nic88). Google Inc. Retrieved January 19, 2021.

244. "Deprecations and removals in Chrome 88" (https://developers.google.com/web/updates/2020/12/chrome-88-deps-rems). Google
Inc. Retrieved January 19, 2021.

245. "Chrome for Android Update" (https://chromereleases.googleblog.com/2021/01/chrome-for-android-update_19.html). January 19,
2021. Retrieved January 20, 2021.

246. Juli Clover (February 11, 2021). "Google Chrome Beta on iOS Lets You Lock Incognito Tabs With Face ID" (https://www.macrumor
s.com/2021/02/11/google-chrome-beta-lock-incognito-tabs/). MacRumors. Retrieved March 3, 2021.

247. Juli Clover (February 10, 2021). "Gmail iOS App Has Out of Date Warning After 2 Months of No Updates as Google Delays
Privacy Labels [Updated]" (https://www.macrumors.com/2021/02/10/gmail-ios-out-of-date-warning/). MacRumors. Retrieved
March 3, 2021.

248. "Stable Channel Update for Desktop" (https://chromereleases.googleblog.com/2021/03/stable-channel-update-for-desktop.html). March 2, 2021. Retrieved March 2, 2021.

249. "New in Chrome 89" (https://developer.chrome.com/blog/new-in-chrome-89/). Google Inc. Retrieved March 2, 2021.

250. "Deprecations and removals in Chrome 89" (https://developer.chrome.com/blog/deps-rems-89/). Google Inc. Retrieved March 2, 2021.

251. "Require SSE3 for Chrome on x86" (https://docs.google.com/document/d/1QUzL4MGNqX4wiLvukUwBf6FdCL35kCDoEJTm2wMkahw/edit#heading=h.7nki9mck5t64). Google Inc. Retrieved March 26, 2021.

252. "Chrome for Android Update" (https://chromereleases.googleblog.com/2021/03/chrome-for-android-update.html). March 2, 2021. Retrieved March 3, 2021.

253. "Stable Channel Update for Desktop" (https://chromereleases.googleblog.com/2021/04/stable-channel-update-for-desktop_14.html). April 14, 2021. Retrieved April 15, 2021.

254. "New in Chrome 90" (https://developer.chrome.com/blog/new-in-chrome-90/). Google Inc. Retrieved April 13, 2021.

255. "Deprecations and removals in Chrome 90" (https://developer.chrome.com/blog/deps-rems-90/). Google Inc. Retrieved April 13, 2021.

256. "Chrome for Android Update" (https://chromereleases.googleblog.com/2021/04/chrome-for-android-update.html). April 13, 2021. Retrieved April 13, 2021.

257. "Chrome for iOS Update" (https://chromereleases.googleblog.com/2021/05/chrome-for-ios-update.html). May 10, 2021. Retrieved May 10, 2021.

258. "Stable Channel Update for Desktop" (https://chromereleases.googleblog.com/2021/05/stable-channel-update-for-desktop_25.html). May 25, 2021. Retrieved May 25, 2021.

259. "New in Chrome 91" (https://developer.chrome.com/blog/new-in-chrome-91/). Google Inc. Retrieved May 26, 2021.

260. "Chrome for Android Update" (https://chromereleases.googleblog.com/2021/05/chrome-for-android-update_01607414128.html). May 25, 2021. Retrieved May 25, 2021.

261. "Chrome for iOS Update" (https://chromereleases.googleblog.com/2021/06/chrome-for-ios-update.html). June 3, 2021. Retrieved June 3, 2021.

262. "[Updated] Want to disable Tab Groups/grid-view in Google Chrome on Android? Here's how to do so" (https://piunikaweb.com/2021/06/14/want-to-disable-tab-groups-grid-view-in-chrome-on-android-heres-how-to-do-so/). June 14, 2021. Retrieved June 14, 2021.

263. "Stable Channel Update for Desktop" (https://chromereleases.googleblog.com/2021/07/stable-channel-update-for-desktop_20.html). July 20, 2021. Retrieved July 20, 2021.

264. "Deprecations and removals in Chrome 92" (https://developer.chrome.com/blog/deps-rems-92/). Google Inc. Retrieved August 31, 2021.

265. "Chrome for Android Update" (https://chromereleases.googleblog.com/2021/07/chrome-for-android-update_01500789893.html). July 20, 2021. Retrieved July 20, 2021.

266. "Chrome for iOS Update" (https://chromereleases.googleblog.com/2021/07/chrome-for-ios-update.html). July 20, 2021. Retrieved July 20, 2021.

267. "Stable Channel Update for Desktop" (https://chromereleases.googleblog.com/2021/08/stable-channel-update-for-desktop_31.html). August 31, 2021. Retrieved August 31, 2021.

268. "New in Chrome 93" (https://developer.chrome.com/blog/new-in-chrome-93/). Google Inc. Retrieved August 31, 2021.

269. "Deprecations and removals in Chrome 93" (https://developer.chrome.com/blog/deps-rems-93/). Google Inc. Retrieved August 31, 2021.

270. "Chrome for Android Update" (https://chromereleases.googleblog.com/2021/08/chrome-for-android-update_0881967577.html). August 31, 2021. Retrieved August 31, 2021.

271. "Chrome for iOS Update" (https://chromereleases.googleblog.com/2021/08/chrome-for-ios-update.html). August 31, 2021. Retrieved August 31, 2021.

272. "Stable Channel Update for Desktop" (https://chromereleases.googleblog.com/2021/09/stable-channel-update-for-desktop_21.html). September 21, 2021. Retrieved September 21, 2021.

273. "New in Chrome 94" (https://developer.chrome.com/blog/new-in-chrome-94/). Google Inc. Retrieved September 24, 2021.

274. "Deprecations and removals in Chrome 94" (https://developer.chrome.com/blog/deps-rems-94/). Google Inc. Retrieved September 21, 2021.

275. "Chrome for Android Update" (https://chromereleases.googleblog.com/2021/09/chrome-for-android-update_21.html). September 21, 2021. Retrieved September 21, 2021.

276. "Chrome for iOS Update" (https://chromereleases.googleblog.com/2021/09/chrome-for-ios-update_21.html). September 21, 2021. Retrieved September 21, 2021.

277. "Stable Channel Update for Desktop" (https://chromereleases.googleblog.com/2021/10/stable-channel-update-for-desktop_19.html). October 19, 2021. Retrieved October 19, 2021.

278. "New in Chrome 95" (https://developer.chrome.com/blog/new-in-chrome-95/). Google Inc. Retrieved October 19, 2021.

279. "Deprecations and removals in Chrome 95" (https://developer.chrome.com/blog/deps-rems-95/). Google Inc. Retrieved October 19, 2021.

280. "Chrome for Android Update" (https://chromereleases.googleblog.com/2021/10/chrome-for-android-update_01703513036.html). October 19, 2021. Retrieved October 19, 2021.

281. "Chrome for iOS Update" (https://chromereleases.googleblog.com/2021/10/chrome-for-ios-update_19.html). October 19, 2021. Retrieved October 19, 2021.

282. "Stable Channel Update for Desktop" (https://chromereleases.googleblog.com/2021/11/stable-channel-update-for-desktop.html). November 15, 2021. Retrieved November 16, 2021.

283. "New in Chrome 96" (https://developer.chrome.com/blog/new-in-chrome-96/). Google Inc. Retrieved November 18, 2021.

284. "Deprecations and removals in Chrome 96" (https://developer.chrome.com/blog/deps-rems-96/). Google Inc. Retrieved November 16, 2021.

285. "Support for Android Lollipop is deprecated in the Chromium code base" (https://groups.google.com/a/chromium.org/g/chromium-dev/c/2MwR9KqwY9I/m/TXLmUL-CAQAJ). Google Groups. November 1, 2021. Retrieved February 8, 2022.

286. "Chrome for Android Update" (https://chromereleases.googleblog.com/2021/11/chrome-for-android-update.html). November 15, 2021. Retrieved November 16, 2021.

287. "Chrome for iOS Update" (https://chromereleases.googleblog.com/2021/11/chrome-for-ios-update.html). November 9, 2021. Retrieved November 9, 2021.

288. "Stable Channel Update for Desktop" (https://chromereleases.googleblog.com/2022/01/stable-channel-update-for-desktop.html). January 4, 2022. Retrieved January 4, 2022.

289. "New in Chrome 97" (https://developer.chrome.com/blog/new-in-chrome-97/). Google Inc. Retrieved January 11, 2022.

290. "Deprecations and removals in Chrome 97" (https://developer.chrome.com/blog/deps-rems-97/). Google Inc. Retrieved January 4, 2022.

291. "Chrome for Android Update [channel mislabeled as "97.0.4664.104"]" (https://chromereleases.googleblog.com/2022/01/chrome-for-android-update.html). January 4, 2022. Retrieved January 4, 2022.

292. "Chrome for iOS Update" (https://chromereleases.googleblog.com/2022/01/chrome-for-ios-update.html). January 4, 2022. Retrieved January 4, 2022.

293. "Stable Channel Update for Desktop" (https://chromereleases.googleblog.com/2022/02/stable-channel-update-for-desktop.html). February 1, 2022. Retrieved February 1, 2022.

294. "New in Chrome 98" (https://developer.chrome.com/blog/new-in-chrome-98/). Google Inc. Retrieved February 1, 2022.

295. "Deprecations and removals in Chrome 98" (https://developer.chrome.com/blog/deps-rems-98/). Google Inc. Retrieved February 1, 2022.

296. "Chrome for Android Update" (https://chromereleases.googleblog.com/2022/02/chrome-for-android-update.html). February 1, 2022. Retrieved February 1, 2022.

297. "Chrome for iOS Update" (https://chromereleases.googleblog.com/2022/02/chrome-for-ios-update.html). February 1, 2022. Retrieved February 1, 2022.

298. "Stable Channel Update for Desktop" (https://chromereleases.googleblog.com/2022/03/stable-channel-update-for-desktop.html). March 1, 2022. Retrieved March 1, 2022.

299. "New in Chrome 99" (https://developer.chrome.com/blog/new-in-chrome-99/). Google Inc. Retrieved March 1, 2022.

300. "Deprecations and removals in Chrome 99" (https://developer.chrome.com/blog/deps-rems-99/). Google Inc. Retrieved March 1, 2022.

301. "Chrome for Android Update" (https://chromereleases.googleblog.com/2022/03/chrome-for-android-update.html). March 1, 2022. Retrieved March 1, 2022.

302. "Chrome for iOS Update" (https://chromereleases.googleblog.com/2022/03/chrome-for-ios-update.html). March 1, 2022. Retrieved March 1, 2022.

303. "Stable Channel Update for Desktop" (https://chromereleases.googleblog.com/2022/03/stable-channel-update-for-desktop_29.html). March 29, 2022. Retrieved March 29, 2022.

304. "New in Chrome 100" (https://developer.chrome.com/blog/new-in-chrome-100/). Google Inc. Retrieved March 28, 2022.

305. "Deprecations and removals in Chrome 100" (https://developer.chrome.com/blog/deps-rems-100/). Google Inc. Retrieved March 20, 2022.

306. "Chrome for Android Update" (https://chromereleases.googleblog.com/2022/03/chrome-for-android-update_0283137014.html). March 29, 2022. Retrieved March 29, 2022.

307. "Chrome for iOS Update" (https://chromereleases.googleblog.com/2022/03/chrome-for-ios-update_29.html). March 29, 2022. Retrieved March 29, 2022.

308. "Stable Channel Update for Desktop" (https://chromereleases.googleblog.com/2022/04/stable-channel-update-for-desktop_26.html). April 26, 2022. Retrieved April 26, 2022.

309. "Deprecations and removals in Chrome 101" (https://developer.chrome.com/blog/deps-rems-101/). Google Inc. Retrieved April 26, 2022.

310. "Chrome for Android Update" (https://chromereleases.googleblog.com/2022/04/chrome-for-android-update_01711927518.html). April 26, 2022. Retrieved April 26, 2022.

311. "Chrome for iOS Update" (https://chromereleases.googleblog.com/2022/04/chrome-for-ios-update_26.html). April 26, 2022. Retrieved April 26, 2022.

312. Pichai, Sundar. "Chrome for Android out of Beta!" (https://chromereleases.googleblog.com/2012/06/chrome-for-android-out-of-beta.html). chrome.blogspot.com. Retrieved June 27, 2012.

313. "The Chromium Blog: A deeper look at Chrome for Android" (https://blog.chromium.org/2012/02/deeper-look-at-chrome-for-android.html). blog.chromium.org. Retrieved February 9, 2012.

314. "Chrome for Android Beta" (https://market.android.com/details?id=com.android.chrome). market.android.com. Retrieved February 9, 2012.

315. "Chrome stops declaring Linux systems obsolete - The H Open: News and Features" (https://web.archive.org/web/201312080227 19/http://www.h-online.com/open/news/item/Chrome-stops-declaring-Linux-systems-obsolete-1803451.html). H-online.com. February 14, 2013. Archived from the original (http://www.h-online.com/open/news/item/Chrome-stops-declaring-Linux-systems-o bsolete-1803451.html) on December 8, 2013. Retrieved March 30, 2013.

External links

- User agent strings (http://www.useragentstring.com/pages/useragentstring.php?name=Chrome) for different versions of Chrome. Archived copy (https://web.archive.org/web/20181114115638/http://www.useragentstring.com/pages/useragentstring.php?name= Chrome).

1. "Chrome Browser release channels - Google Chrome Enterprise Help" (https://support.google.com/chrome/a/answer/9027636?hl =en&ref_topic=9023448). *Google Support*. Google Inc. Retrieved December 7, 2018.

2. Ryan Benson (October 2, 2013). "History Index files removed from Chrome v30" (https://dfir.blog/history-index-files-removed-from-chrome-v30/). Retrieved March 14, 2022.

3. Benson, Ryan. "Archived History files removed from Chrome v37" (https://web.archive.org/web/20141010125418/http://www.obsid ianforensics.com/blog/archived-history-files-removed-from-chrome-v37/). Obsidian Forensics. Archived from the original (http://ww w.obsidianforensics.com/blog/archived-history-files-removed-from-chrome-v37/) on October 10, 2014. Retrieved October 27, 2021.

4. "[chrome] Revision 275159" (https://src.chromium.org/viewvc/chrome?revision=275159&view=revision). *src.chromium.org*. Retrieved October 27, 2021.

5. "Shadow DOM v1 - Chrome Platform Status" (https://www.chromestatus.com/feature/4667415417847808).

6. "Background Tabs in Chrome 57 | Web | Google Developers" (https://developers.google.com/web/updates/2017/03/background_t abs). *Google Developers*. Retrieved April 26, 2017.

7. "Audio/Video Updates in Chrome 63/64 | Web" (https://developers.google.com/web/updates/2017/12/chrome-63-64-media-update s). *Google Developers*. Retrieved June 4, 2021.

8. "Chrome 64 for Android cuts URLs automatically when you share them", GHacks, February 20th 2018 (https://www.ghacks.net/20 18/02/20/chrome-64-for-android-cuts-urls-automatically-when-you-share-them/)

9. "Chrome actualiza su modo incógnito: adiós a las capturas de pantalla" (https://www.adslzone.net/2018/03/26/chrome-65-incognit o-capturas/). *ADSLZone* (in European Spanish). March 26, 2018. Retrieved August 4, 2018.

10. "Google Chrome for Android is dropping support for Android 4.1-4.3 Jelly Bean" (https://www.xda-developers.com/google-chrome-android-dropping-support-android-4-1-4-3-jelly-bean/). XDA Developers. October 5, 2018. Retrieved December 10, 2018.

11. "Issue 1076521: Some Automatic Lazy Loading Breaks Existing Javascript Lightboxes" (https://bugs.chromium.org/p/chromium/is sues/detail?id=1076521&q=lightbox%20os=Windows&can=2&sort=modified). *bugs.chromium.org*. April 29, 2020. Retrieved August 17, 2020.

12. "Chrome can now caption audio and video" (https://blog.google/products/chrome/live-caption-chrome/). *Google*. March 18, 2021. Retrieved April 3, 2021.

13. Campbell, Ian Carlos (March 17, 2021). "Chrome now instantly captions audio and video on the web" (https://www.theverge.com/2 021/3/17/22337074/chrome-real-time-live-captions-audio-accessibility). *The Verge*. Retrieved April 3, 2021.

14. "Chrome 59 Stable Channel Update for Desktop" (https://chromereleases.googleblog.com/2017/06/stable-channel-update-for-des ktop.html). *Chrome Releases*. June 5, 2017. Retrieved August 21, 2017.

Brown v. Google

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA

CHASOM BROWN, WILLIAM BYATT, JEREMY DAVIS, CHRISTOPHER CASTILLO, and MONIQUE TRUJILLO, individually and on behalf of all similarly situated,
 	
    Plaintiffs,
            v.
 	
GOOGLE LLC,
 	
    Defendant.
	§ §	**Case No. 4:20-cv-03664-YGR-SVK**

EXPERT REBUTTAL REPORT OF BRUCE SCHNEIER

REBUTTAL OF EXPERT GEORGIOS ZERVAS

APPENDIX 2

June 7, 2022

Brown v. Google

- **GOOG-CABR-04665130**: An April 22, 2014 article in *The Guardian*.
  - This article does not even mention the words "private" or "Incognito," or discuss Google's collection and use of private browsing information.
- **GOOG-CABR-04665136**: A September 2018 user discussion thread on the Hacker News website.
  - None of the comments refer to Google's collection of private browsing information; rather, the users are discussing Chrome Sync mode.
- **GOOG-CABR-04665141**: A November 2019 article on MetaBlog.
  - This article replicates Google's misleading Splash Screen text: "[y]our Internet Service Provider, your employer, the government or any of the websites you've visited can still track your browsing activities." As on the Splash Screen, Google is omitted from the list.
- **GOOG-CABR-04665148**: A December 2015 paper in the *International Journal of Computer Applications*.
  - This paper describes an experiment in which researchers "examine[d] the artifacts left in main memory after a private browsing session," that is, private browsing information stored on a user's device. The study does not consider whether private browsing data is collected and then stored by third parties such as Google.
  - This study actually undermines Professor Zervas's conclusion that the use of a private browsing mode "prevent[s] browsing history from being saved on the device",[1] given its conclusion that "private browsing mode does leave browsing evidence even after the browsers were closed in all four web browsers under this experiment"—specifically, Firefox, Internet Explorer, Safari, and Chrome Incognito.
- **GOOG-CABR-04665156**: A September 2016 article in *Bustle*.
  - This article notes that "Incognito mode doesn't offer complete privacy," but otherwise restates Google's misleading disclosures, explaining that the user's browsing history is still available to their ISP and employer. There is no discussion of Google's tracking beacons.
- **GOOG-CABR-04665164**: A 2016 report from the 2016 CHI Conference.
  - This article summarizes focus groups in which participants provided rationales for their online behavior. One participant stated that "I will use [] Incognito mode because it makes me feel better. Although I'm sure that [Google] can still track something." (second alteration in original). This statement provides no evidence that the participant knew that Google uses tracking beacons embedded within non-Google websites to collect his or her browsing information, nor that Google tags this data with Incognito detection bits and stores it such that it can be linked to his or her identity.
- **GOOG-CABR-04665171**: An undated article from independent.co.uk.
  - This repeats Google's misleading Splash Screen text, warning that "your boss could figure out if you're doing something you're not supposed to at work," with no mention of Google's tracking beacons.
- **GOOG-CABR-04665175**: An August 2018 article in the *New York Post*.
  - This discusses the privacy risk to users who sign in to Google during an Incognito session, warning that "If you log back into Google before leaving Incognito

---

[1] Zervas Report ¶ 5.

Brown v. Google

Mode, Google will be able to retroactively link your browsing data to your account […] The only way to get around this would be to only log into your Google account after you've left Incognito Mode." The article thus suggests to users that Google cannot collect and store their private browsing information when they are signed out of Google.

- **GOOG-CABR-04665178**: An April 2019 article on indy100.com.
  - o This restates Google's misleading Splash Screen disclosures, noting that Incognito mode "has little effect on your ISP and whichever sites you visit being able to follow your activity."
- **GOOG-CABR-046651863**: An April 2019 article in *Cosmopolitan*.
  - o Like the *New York Post* item discussed above, this warns of the privacy risk to users who sign in to Google while browsing within Incognito, explaining that "Google can still record the websites you browse while in Incognito mode on the Chrome browser and link them to your identity, *if* you're logged into your Google account." (emphasis in original)
- **GOOG-CABR-04665190**: Introduction to an August 2018 blog post on the *Wired* website.
  - o This simply states Google has made a change to Chrome whereby Chrome appears to "log people in" without permission; it makes no mention of Chrome Incognito or any private browsing mode.
- **GOOG-CABR-04665192**: A May 2018 article from *Fast Company*.
  - o This advocates for Firefox as opposed to the Chrome browser, but does not discuss Google's collection of users' browsing information from visits to non-Google websites within Incognito mode. Although it advises that "Chrome allows third-party websites to access your IP address and any information that site has tracked using cookies," it does not explain that Google can be one of these websites.
- **GOOG-CABR-04665201**: A September 2018 article from the BBC.
  - o This discusses selling one's personal data, stating that "the reason our data is so lucrative for big companies is the volumes they are able to scoop up – billions of users feed their algorithms every day . . . But me? I doubt I'll ever be able to make more than a few dollars a month [from selling my data]." The article does not cover the means by which Google obtains, stores and monetizes information, whether users are browsing in regular or Incognito mode, nor disclose that Google collects private browsing information. The article does, however, capture why data is so valuable to Google, including by noting that it "feed[s] their algorithms."
- **GOOG-CABR-04665206**: An archived copy of the Chick-fil-A home page (http://www.chick-fil-a.com).
  - o This displays Chick-fil-A's cookie policy, stating that "cookies on this site are used by Chick-fil-A and our advertising and analytic partners for different purposes, including personalizing content, tailoring advertising to your interests, and measuring site usage. By continuing, you agree to our use of cookies." It does not disclose that any of its "advertising and analytic partners" will collect private browsing information.

Brown v. Google

- **GOOG-CABR-04665212**: Creative People Crew home page (partners.cpeople.ru).
  - This page displays the following cookie policy: "you agree to process cookies and your personal data: location; OS type and version; browser type; device; visited pages on the site; IP-address." The page says nothing about Google, private browsing, or Google's collection, storage and use of users' private browsing information.
- **GOOG-CABR-04665217**: A December 2017 article on the website of television station WKYC, syndicated from *USA Today*.
  - This makes no mention of Chrome Incognito or any other private browsing mode, and incorrectly suggests to users that they can keep track of and view all of the information that Google has collected about them. Google does not permit users to access or delete the information collected from their private browsing sessions.
- **GOOG-CABR-04665225**: Didomi.io's Consent Management Platform.
  - This page says nothing about Google or its collection of private browsing information.
- **GOOG-CABR-04665238**: An October 2019 article on the PäksTech website.
  - This only discusses Firefox, and makes no mention of Chrome's Incognito mode.
- **GOOG-CABR-04665244**: A Question and Answer page on Quora, spanning eleven years from 2011 to 2022.
  - This is a discussion of whether "Google track[s] what happens in the 'incognito window.'" Eighteen visitors weigh in on the question. One Google Chrome employee commented that "Google does not track your non-incognito use of Chrome" and that "rather Chrome sends search terms typed into the omnibox to the search provider of your choice." This Google employee was either himself misinformed or misled the discussion participants with his suggestion that Google does not even track users within a regular browsing mode. None of the 18 commenters discuss the means by which Google tracking beacons embedded within non-Google websites will collect information about users' private browsing while they are signed out of Google.
- **GOOG-CABR-04665250**: An August 2018 article from *The Atlantic*.
  - This briefly refers to a 2018 Vanderbilt University study involving a scenario in which the user signs into Gmail while privately browsing.[2]
- **GOOG-CABR-04665613**: A customer service and privacy policy page from PUMA.com.
  - This page establishes that PUMA.com uses Google Analytics but says nothing about Google Analytics tracking beacons or private browsing modes.
- **GOOG-CABR-04665621**: A September 2019 article from *PC Magazine*.
  - This article states that "Your ISP, corporate network administrator, and government agencies will be able to track your browsing habits regardless of the browsing mode you're using." Although it also notes that "websites can still discover your identity" while private browsing, it does not explain that Google can do so even when a user visits a non-Google website while signed out of their Google account and using a private browsing mode.

---

[2] Douglas C. Schmidt, "Google data collection," Vanderbilt University, https://digitalcontentnext.org/wp-content/uploads/2018/08/DCN-Google-Data-Collection-Paper.pdf (August 15, 2018).

Brown v. Google

- **GOOG-CABR-04665630**: A page from PUMA.com displaying a cookie policy pop-up.
  - This statement says nothing about Google or its collection of private browsing information.
- **GOOG-CABR-04665638**: A July 2018 article from *Digital Information World*.
  - The article discusses a recent study that sought to ascertain users' beliefs about private browsing modes. The research found that "people incorrectly assumed that incognito mode was capable of doing much more than what it can actually do," an assumption that supports my opinion that Google's disclosures are misleading. The article says nothing about Google's collection of private browsing information.
- **GOOG-CABR-04665641**: The *Scientific American* website's privacy policy.
  - The policy states that the website uses Google services but mentions neither private browsing nor Google's collection of private browsing information.
- **GOOG-CABR-04665673**: A position paper by Christopher Soghoian for the December 2010 IAB Internet Privacy Workshop.
  - This paper contends that users do not understand that private browsing modes do not prevent information from being sent to a user's ISP or employer, and credits Google for making that clear on the Incognito Splash Screen. However, the article does not discuss Google's collection of private browsing information from users' visits to non-Google websites.
- **GOOG-CABR-04665676**: A screenshot from the Starbucks website displaying its cookie policy and cookie settings options.
  - No mention is made of Google, private browsing, or Google's collection of private browsing information.
- **GOOG-CABR-04665682**: A discussion thread on *Hacker News* beginning on September 8, 2018.
  - This long discussion focuses on Google requiring Gmail users to log into Chrome. No mention is made of Google's collection of private browsing information from signed out browsing sessions.
- **GOOG-CABR-04665705**: A November 2018 article from *Wired*.
  - This article discusses Google's approaches to user privacy over the years, but not Google's collection of private browsing information.
- **GOOG-CABR-04665712**: A July 2018 article from *Yahoo Finance*.
  - This piece summarizes the same study as the above-described July 2018 article from *Digital Information World*,[3] and supports my opinion that users harbor "a lot of misconceptions about browsing the web in 'incognito' mode." But like the *Digital Information World* piece, it does not mention Google's collection of private browsing information from non-Google websites.
- **GOOG-CABR-04665718**: A July 2019 article from *Mashable*.
  - This article discusses trackers on websites but does not consider the possibility that Google can be one of these trackers, or that Google collects information about users' private browsing activities on non-Google websites.

---

[3] GOOG-CABR-04665638

Brown v. Google

- **GOOG-CABR-04665727**: The Weather.com user privacy pop-up.
  - Google is nowhere mentioned, let alone its collection of private browsing information.
- **GOOG-CABR-04665732**: A December 2017 article from CNBC.
  - The describes various types of information that Google routinely collects from users, and directs readers who wish to limit collection of data to various locations on the Google website where they can change their privacy settings. The article does not say anything about private browsing mode, let alone that Google collects private browsing information.
- **GOOG-CABR-04665750**: An article from *Forbes Advisor*, last updated on August 9, 2021.
  - This article discusses the collection of information by websites you visit, including search engines, but does not touch upon Google's collection of information from private browsing sessions.
- **GOOG-CABR-04665756**: A November 2017 article from *Thrillist*, based on an interview with Darin Fisher, Google's Vice-President of Chrome.
  - This article supports my opinion, in that Fisher discloses that Google employees ["k]now that Incognito Mode is still widely misunderstood," and that "the Chrome team agonized over what to call it in the beginning, intentionally steering away from including 'privacy' in the name, because it didn't want to oversell its ability." However, Fisher furthers that misunderstanding by citing to the misleading Splash Screen disclosures, without acknowledging that Google collects users' private browsing information.
- **GOOG-CABR-04665766**: A June 2018 article from Consumer Reports.
  - This article addresses various user misconceptions regarding Incognito mode, and mentions Google's ability to record search history when users are logged into Google within a private browsing mode, but does not disclose Google's collection of private browsing data from non-Google websites.
- **GOOG-CABR-04665773**: A February 2014 article from *Life Hacker*.
  - This article discusses how Google collects personal information, asserting that "Chrome isn't a primary source of any of it. Gmail, your Google Search history, your YouTube account, your Google+ account, the files you store on Google Drive, and other browser-independent features are where your data really comes from." The article says nothing about Google's collection of private browsing information.
- **GOOG-CABR-04665791**: An April 2018 article from the *Wall Street Journal*.
  - This article discusses Google Analytics tracking; however no reference is made to Incognito mode or other private browsing modes, or about Google's collection of private browsing information.
- **GOOG-CABR-04665797**: A September 2018 blog post on *Cryptography Engineering* and its associated discussion thread.
  - This blog post, titled "Why I'm Done with Chrome," concerns the automatic log-in feature introduced to Chrome in 2018. Some comments mention Incognito mode, but none discuss it beyond using it as a means to avoid giving information to Google, thus supporting my opinion.

Brown v. Google

- **GOOG-CABR-04665836**: An April 2020 article from *Slate*.
  - o This discusses whether users should be able to monetize their data. It does not address private browsing or Google's collection of private browsing data.
- **GOOG-CABR-04665840**: A Zoom explanatory sales pitch file.
  - o This is a brief explanation of very basic Zoom services with no references to Google at all, only a pop-up at the bottom of the page offering users the opportunity to opt out of third-party cookies and ad retargeting.
- **GOOG-CABR-05876970**: A September 2013 article on *Slate*.
  - o This article mentions neither Incognito mode nor private browsing modes in general. Although it notes that Google receives information about users' visits to "more than 88 percent of websites," it says nothing about whether Google collects and stores users' browsing information when they choose to use Incognito mode.
- **GOOG-CABR-05876977**: A December 2019 blog post on the website of Bounteous, a digital marketing company.
  - o This article discusses Google Analytics tracking, and explains how the Analytics User ID "can be used to stitch sessions and users across browsers and devices." Neither Incognito nor any other private browsing mode are mentioned, nor is the fact that Google tracks users via analytics tracking beacons even within a private browsing session.
- **GOOG-CABR-05876987**: A February 2014 article from *Lifehacker*.
  - o This article discusses Google Chrome yet says nothing about Chrome Incognito or any other private browsing mode. This article also supports my opinions on joinability, with its explanation that "'non-personally identifiable data' often really isn't at all."
- **GOOG-CABR-05877005**: This is the same *Wall Street Journal* article as GOOG-CABR-04665791.
- **GOOG-CABR-05877011**: An August 2018 article on CNN.
  - o This report on the 2018 Vanderbilt University study[4] discusses Google's extensive data collection practices yet says nothing about Incognito or about Google's collection of private browsing information.
- **GOOG-CABR-05877015**: A February 2020 article from *The Register*.
  - o This article describes Google's receipt of the X-Client Data Header, which is not sent during an Incognito browsing session. The author does not discuss whether Google receives any information from users' private browsing sessions, but nonetheless correctly notes that "Google . . . can still ID everyone it wants."
- **GOOG-CABR-05877023**: A May 2018 article on *Fast Company*.
  - o The article contains a single mention of Incognito mode, referring to "data leakage" from Chrome Incognito; the author does not specify what sort of "data leakage" she means, or how that data is leaked. The article undermines Professor Zervas's opinions about the settings and features that he claims will block Google's tracking beacons, explaining that "Chrome settings that don't encourage privacy are the default" and pointing out that "Settings pages aren't a good UX solution to providing clear information about how data is used . . . because who really spends any time in their privacy settings."

---

[4] Douglas C. Schmidt, "Google data collection," Vanderbilt University, https://digitalcontentnext.org/wp-content/uploads/2018/08/DCN-Google-Data-Collection-Paper.pdf (August 15, 2018).

Brown v. Google

- **GOOG-CABR-05877032**: This document contains two articles from the WKYC website.
  - One is about the first Harry Potter book. I have read that book, and it does not disclose Google's collection of private browsing data.
  - The other is the same syndicated *USA Today* piece featured in GOOG-CABR-04665217.
- **GOOG-CABR-05877040**: A July 2019 article on Clark.com
  - This article discusses the "Do Not Track" setting, and says nothing about any private browsing mode.
- **GOOG-CABR-05877049**: This is an undated article about DuckDuckGo from http://www.spreadprivacy.com.
  - This author discusses the "Myth of Incognito Mode," explaining that it "does not offer any additional protection as preventing the websites you visit from collecting your information" and warning that "Google is still tracking your searches." However, the tracking at issue in this case pertains not to searches on Google.com, but to the browsing activity of signed-out Incognito users.
- **GOOG-CABR-05877056**: A screenshot from Macys.com.
  - Here, Macy's informs visitors that "We also share information about your use of our site with our social media, advertising, and analytics partners." Google is nowhere mentioned, nor are any private browsing modes.
- **GOOG-CABR-05877221**: An October 2021 article from *Reader's Digest*.
  - This article discusses Google's Web & App activity feature, and does not discuss private browsing.
- **GOOG-CABR-05877233**: This is an August 2020 article on *Wired*.
  - This article discusses what happens when someone signs into Google while using Incognito, explaining that "your searches are once again being logged and associated with your account." The article also warns that when you don't sign in, "the websites that you visit . . . figure out who you might be." The article does not disclose that Google collects information about users' private browsing on non-Google websites while signed out of their Google account.
- **GOOG-CABR-05877325**: This is the same *Wired* article as GOOG-CABR-05877233.
- **GOOG-CABR-05877511**: An April 2021 article on *Insight*.
  - The *Insight* article discusses this lawsuit, noting that "Google has been sued in California because it continues to track people's data even in the Chrome browser's Incognito mode. Did that send a chill down your spine?" The author appears to agree with Plaintiffs' allegations and my opinions regarding Incognito's misleading branding: "The name incognito has been etched in our minds in such a way that we instantly relate it to complete data privacy, that anything you do online via the Chrome browser will not be tracked, but now we know that it's not all true."
- **GOOG-CABR-05877813**: A July 31, 2020 article, apparently from *Fast Company*.
  - The article refers to this lawsuit ("a recent lawsuit against Google alleges that internet users are not getting the privacy protection they expect when using Chrome's Incognito mode"), and supports my opinions regarding Incognito's misleading branding ("It is not all that surprising that people have misconceptions about how private browsing mode works; the word "private" suggests a lot more protection than these modes actually provide. […] it may be difficult to dispel all of these myths without changing the name of the browsing mode").

Brown v. Google

- **GOOG-CABR-04665260**: A 2019 article from *Inc*.
  - This article merely quotes Google's "fine print," stating that in Incognito, "downloads and bookmarks will be saved" and "activity might be visible to: Websites you visit, your employee or school, your internet service provider." Google itself is omitted from this list.
- **GOOG-CABR-04665266**: This is the same article from indy100.com as GOOG-CABR-04665178.
- **GOOG-CABR-04665270**: This is the same article from Clark.com as GOOG-CABR-05877040.
- **GOOG-CABR-04665279**: An August 2018 article from *The Independent*.
  - The pdf contains the first two sentences of a report[5] (the remainder blocked by a log-in request) on the 2018 Vanderbilt University study of Google's data collection,[6] describing the study's finding that "Google could retroactively link a person's private browsing to the usernames and account information they use online." Even though most of the *Independent* piece is missing from the pdf, I am familiar with the Vanderbilt study, which involved a scenario in which the user signs into Gmail while privately browsing. The Vanderbilt study does not discuss Google's collection and storage of private browsing data even from users' signed-out sessions, data that can be linked to individual users.
- **GOOG-CABR-04665283**: A July 2019 article from *Wired UK*.
  - This article notes that the websites might be able to detect that you are Incognito, including for purposes of enforcing paywalls. The article does not note that Google tracking beacons embedded within non-Google websites will continue to operate regardless of whether the user is in a private browsing mode.
- **GOOG-CABR-04665287**: A November 2017 article from *Huffington Post UK*.
  - This article points to the fact that Incognito is "absolutely not going to be keeping your employer from seeing what you do" and cautions users against using Incognito "to mix business with personal at work." No mention is made of Google's practice of tracking users' Incognito browsing activity.
- **GOOG-CABR-04665294**: An October 2016 article from ProPublica.
  - This article discusses Google's new language in its general Privacy Policy, disclosing that "your activity on other sites and apps may be associated with your personal information in order to improve Google's services and the ads delivered by Google." No reference is made to Incognito or private browsing.
- **GOOG-CABR-04665298**: An April 2019 article from *The Australian*.
  - This piece quotes from a letter to the US House of Representatives judiciary committee from Sundar Pichai: "When a user conducts a search on Google in Chrome Incognito and signed-out modes, we set a cookie to correlate searches conducted in the same Incognito window during the same browsing session. We will, however, use certain factors … such as the browser type, language, time of

---

[5] Anthony Cuthbertson, "Google Chrome's private incognito mode leaks way more personal data than you might think," *The Independent*, https://www.independent.co.uk/tech/google-chrome-incognito-mode-personal-data-private-browser-a8502386.html (August 22, 2018).

[6] Douglas C. Schmidt, "Google data collection," Vanderbilt University, https://digitalcontentnext.org/wp-content/uploads/2018/08/DCN-Google-Data-Collection-Paper.pdf (August 15, 2018).

Brown v. Google

search, location (or an estimation of location), and prior browser session searches, to improve search ranking relevance for the user's query." Pichai's limited mention of Incognito is thus confined to Google Search, without any mention of Google's tracking of Incognito users' visits to non-Google websites.

- **GOOG-CABR-04665305**: An October 2018 article from *Slate*.
  - o This article discusses Google's then-new "feature" of automatically logging Chrome users in to their accounts, the tech community's response, and how this development indicated that Google might be "increasingly trading away [users'] trust for short-term benefits." No mention is made of Incognito or private browsing.
- **GOOG-CABR-04665310**: An October 2018 article from *Wired*.
  - o Like the August 2018 Independent piece, this pdf contains only the first two sentences of the article, with the rest blocked by a paywall. These two sentences simply state that in response to "mounting criticism," Google has developed a "new tool […] to make it easier for you to understand what data Google collects, and surface the choices you have to control it."
- **GOOG-CABR-04665312**: A September 2018 article from *Forbes*.
  - o This article, like GOOG-CABR-04665797 and GOOG-CABR-4665305, also discusses the update that logged users into Chrome "every time a user signed into a Google service," and also includes no reference to Incognito or private browsing.
- **GOOG-CABR-04665316**: A November 2017 article from *Metro News*.
  - o This article simply reiterates Google's misleading Splash Screen text stating that "Google incognito doesn't hide browsing from your employer, your internet service provider, or the websites you visit." No reference is made to Google itself tracking your activity in any capacity.
- **GOOG-CABR-04665328**: A March 2020 article from the Electronic Frontier Foundation.
  - o This article discusses how Google monetizes data without "selling" it for the purposes of the California Consumer Privacy Act, and makes no mention of Incognito or private browsing.
- **GOOG-CABR-04665341**: This is a March 2020 article from *The Register*.
  - o This article is a follow-up to GOOG-CABR-05877015, further discussing the X-Client Data Header. The article does not discuss Incognito or private browsing in any capacity.
- **GOOG-CABR-04665347**: This is the same article from the *New York Post* as GOOG-CABR-04665175.
- **GOOG-CABR-04665356**: This is the same CNN article as GOOG-CABR-05877011.
- **GOOG-CABR-04665360**: An August 2018 article from *The Sun*.
  - o This report on the 2018 Vanderbilt University study states that "Google could see information from before you logged in, but while you were in Incognito Mode – and link it to your Google identity" and "[t]he only way to get around this would be to only log into your Google account after you've left Incognito Mode." The author thus inaccurately suggests that Google does not collect private browsing information when users are signed out of Google.
  - o Moreover, the article describes how Google discredited the study. A "Google spokesperson said: 'This report is commissioned by a professional DC lobbyist group, and written by a witness for Oracle in their ongoing copyright litigation

Brown v. Google

with Google. So it's no surprise that it contains wildly misleading information.'" It makes no sense for Google to now rely on a study that Google at the time described as "wildly misleading."

- **GOOG-CABR-04665372**: This is the same DuckDuckGo article as GOOG-CABR-05877049.
- **GOOG-CABR-04665379**: This is the same article from the Bounteous website as GOOG-CABR-05876977.
- **GOOG-CABR-04665389**: A May 2018 article from *Unsearcher*.
  - The main focus of this article is Google's tracking of Safari users, noting that "Google has also started to set an advertising cookie from its Google.com domain" and that it is "only setting this cookie on Safari browser" as a method of "bypassing Safari tracking protection." No mention of Chrome is made at all, let alone Incognito or any private browsing mode.
- **GOOG-CABR-04665392**: This is the same article from *Slate* as GOOG-CABR-05876970.
- **GOOG-CABR-04665399**: A June 2013 article from *Financial Times*.
  - The article presents an interactive "calculator" to check how much the "multibillion-dollar data broker industry" will pay for a person's data. There is no mention of private browsing mode or Incognito, Google's data collection practices, or Google's collection of private browsing information.
- **GOOG-CABR-04665403**: A July 2017 article from *How-To Geek*.
  - This article states that private browsing modes "offer some improved privacy, but it's not a silver bullet that makes you completely anonymous online." The article notes that an ISP, school, or employer might be able to see one's private browsing data, but does not refer to Google's collection or use of private browsing information.
- **GOOG-CABR-04665410**: A November 2019 article from *Lifehacker*.
  - The article discusses Google's extensive data collection practices and credits Google for offering users "greater control over the ultimate fate of the data it collects." There is no discussion of Incognito mode, of private browsing mode generally, or of Google's collection of private browsing information.
- **GOOG-CABR-04665415**: A May 2020 article from *Lifehacker*.
  - This article briefly discusses Google's newly-announced plan to begin blocking third-party cookies in Incognito mode. However, the article nowhere discusses Google's collection of private browsing information by means of Google tracking beacons embedded within non-Google websites.
- **GOOG-CABR-04665437**: A June 2021 article from *Consumer Reports*.
  - This article describes Google's various "controls and techniques," such as the Web & App Activity control, but makes no mention of Incognito or any other private browsing mode.
- **GOOG-CABR-04665452**: A November 2017 article from *The Sun*.
  - The article echoes Google's assurances that Incognito does not hide your browsing from your employer, ISP, or websites that you visit; however, it reveals nothing about Google's collection and use of private browsing information.

Brown v. Google

- **GOOG-CABR-04665461**: A November 2017 article from *The Independent*.
  - o Like the above-mentioned article, this item merely reiterates that by using Incognito mode, a user's private browsing activity is not hidden from their employer if they are using their work computer.
- **GOOG-CABR-04665467**: An undated article from *United States Cybersecurity Magazine* titled "Incognito Mode: Are you Really Incognito?"
  - o This article notes that "you can still leave a trace on your Google account if you log in during Incognito mode use," but does not discuss Google's collection of information from Incognito sessions even when the user is signed out of Google.
- **GOOG-CABR-04665473**: This is the same article from *The Register* as GOOG-CABR-05877015.
- **GOOG-CABR-04665481**: An October 14 article from *Guiding Tech*.
  - o This article merely states that your browsing history is still available to your employer, ISP, and websites that you visit. Moreover, the article inaccurately suggests that Incognito mode is "good for" "hid[ing] your interactions with the internet from . . . the Google account you're logged into." The article does not mention the fact that Google tracking beacons will enable Google to collect information from users' visits to non-Google websites using a private browsing mode.
- **GOOG-CABR-04665490**: A December 2018 article from *Wired*.
  - o The article does not mention private browsing, Incognito mode, or Google's collection of private browsing data.
- **GOOG-CABR-04665494**: A screenshot of the "Notice of Privacy Practices" on macys.com (updated in June 2021).
  - o Here, Macy's informs users that "Macy's shares data with Google Analytics . . . to understand and optimize website performance and enhance site usability" for its customers and also states that "Google Analytics may associate and group session visits to [Macy's] website from various browsers and devices." This Notice, however, does not discuss Incognito mode, Google's collection of private browsing information, or the fact that Google Analytics tracking beacons continue to operate even when a visitor is using a private browsing mode.
- **GOOG-CABR-04665515**: This is the same screenshot from Macys.com as GOOG-CABR-05877056.
- **GOOG-CABR-04665523**: A September 2018 article from *Unsearcher*.
  - o This article discusses the X-Client Data Header, which is not sent during an Incognito browsing session, but says nothing about Google's collection of private browsing information.
- **GOOG-CABR-04665528**: A June 2019 article from *UpBuild*.
  - o This article discusses Mozilla Firefox's blocking of third-party cookies, but mentions nothing about Incognito mode or private browsing mode more generally.
- **GOOG-CABR-04665548**: A February 2017 article from *Ars Technica.*
  - o This article does not discuss Incognito mode, private browsing, or Google's collection of private browsing information. Incognito is mentioned in a single "Promoted Comment" at the end of the post; the commenter describes a visit to "the uniquemachine.org tracker," which reportedly detected the same "computer fingerprint" for both Chrome and Chrome Incognito windows.

Brown v. Google

- **GOOG-CABR-04665556**: A 2017 paper by Graeme Horsman, University of Sunderland, titled "A process-level analysis of private browsing behavior: A focus on Google Chromes Incognito Mode."
    - This study focuses on "what is occurring on a local system during a private browsing session," tested in an experiment in which researchers sought to identify "where local disk writes occur during a private browsing session." The researchers did not ascertain whether private browsing data is collected and stored by third parties, such as Google.
- **GOOG-CABR-04665563**: A screenshot of the "Privacy Policy" from The Weather Channel (weather.com).
    - The Weather Channel's "Privacy Policy" informs users that "[w]hen your data is collected on the Services, it may be shared with select Analytics Vendors and Advertising Vendors that assist us with marketing or advertising campaigns for our brands, and providers of services that assist us with our business operations with the provision of the Services, or in delivering you the features and functionality that you have requested." There is no discussion of Incognito or private browsing mode within the policy. Moreover, the Policy notes that "this Privacy Policy does not cover the practices of our vendors outside of our Services and we do not control our vendors' technologies."